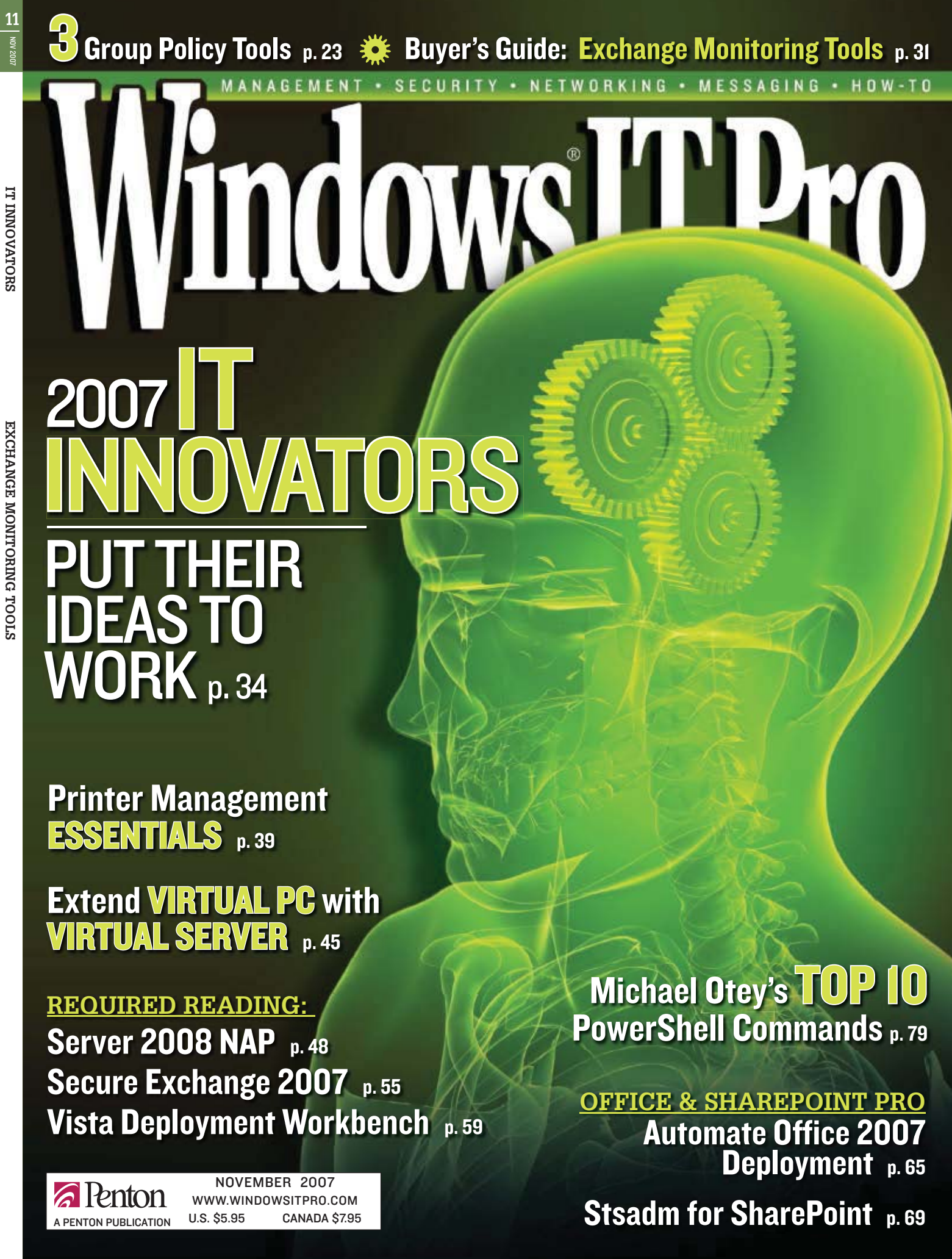
3 Group Policy Tools p. 23

Buyer's Guide: Exchange Monitoring Tools p. 31

MANAGEMENT • SECURITY • NETWORKING • MESSAGING • HOW-TO

Windows® IT Pro



2007 IT INNOVATORS PUT THEIR IDEAS TO WORK p. 34

Printer Management ESSENTIALS p. 39

Extend VIRTUAL PC with VIRTUAL SERVER p. 45

REQUIRED READING:

Server 2008 NAP p. 48

Secure Exchange 2007 p. 55

Vista Deployment Workbench p. 59

Michael Otey's TOP 10 PowerShell Commands p. 79

OFFICE & SHAREPOINT PRO

Automate Office 2007 Deployment p. 65

Stsadm for SharePoint p. 69

Penton
A PENTON PUBLICATION

NOVEMBER 2007
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

_INFRASTRUCTURE LOG

_DAY 84: Feeling really disconnected. We're not getting the most out of our existing assets. Service and application integration is a nightmare. Our connections are restrictive. We've got to stop working on these islands.

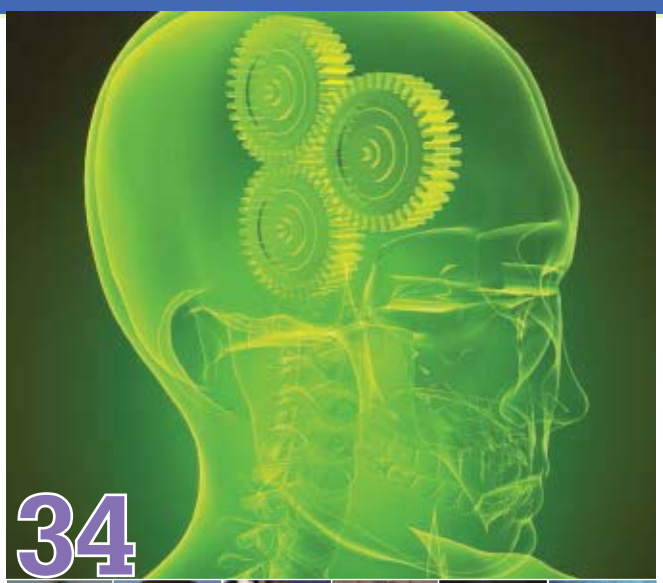
_Please rescue me from this lack of connectivity.

_DAY 87: I've taken back control with IBM WebSphere solutions. Now we can service-enable and connect our existing assets for mission-critical goals. We can reuse existing applications and save money by eliminating redundant systems. Now we're ready for any SOA integration project.

_Plus, no more jellyfish stings.

Download the enterprise service bus white paper at:
IBM.COM/**TAKEBACKCONTROL**/CONNECT

Windows IT Pro
NOVEMBER 2007 VOLUME 13 NO. 11



COVER STORY

FEATURES

FEATURES

REQUIRED READING: SECURITY
SOLUTIONS+

REQUIRED READING: EXCHANGE SERVER

REQUIRED READING: WINDOWS VISTA

OFFICE & SHAREPOINT PRO

COLUMNS

COVER PHOTO BY

Access articles online at www.windowsitpro.com. Enter the article ID in the InstantDoc ID text box.

"Thinstall has made it much easier for us to deploy and move different versions of software throughout our organization."

—Serge Bedard, technology architect specialist

TRICKS & TRAPS

PRODUCTS

WHAT'S HOT

IN EVERY ISSUE

Mark Minasi
Windows Power Tools
The Final For
In this last of three For columns, learn how the tool's /f option lets you tell Windows to apply a single command to a specific list of files.
InstantDoc ID 96903

Michael Otey
Top 10
Essential Windows PowerShell Commands
Windows PowerShell is the wave of the future of Windows scripting. These commands get you started performing basic tasks such as reading or writing to a file, starting a debugger, and retrieving Windows event logs.
InstantDoc ID 96954

88

Learning Path Article not a perfect fit? Find more resources to match your knowledge and skills.
Interact! Network with authors, peers, product vendors, and Microsoft.

It's a small world after all...

Your organization is global and so is your IT infrastructure. Some days that means you need to operate and solve problems in 12 time zones. With Avocent, you can solve most any crisis that the network gremlins can throw at you without leaving your desk or using your passport.

Avocent infrastructure solutions put complete manageability at your fingertips. We've combined our innovative and powerful hardware and easy-to-use software to enable remote access and control of literally any system on the planet. At anytime. From anywhere.

Download our white paper today and find out how you can manage your physical and virtual world from one common interface. Visit **www.avocent.com/itpro**

Avocent®

YEAH, WE'RE WORKING ON THAT

YOUR SAVVY ASSISTANT

The Missing Link to IT Resources

by Christan Humphries

Can You Hear Me Roar Now?

In her 1970s hit, Helen Reddy proclaimed that women were roaring in "numbers too big to ignore." But from where I stand, I can hardly detect a purr from the women in IT. Men send in their What's Hot picks, write Reader to Reader tips, and sometimes even appear on the cover. This month's cover story (page 34) highlights community innovators, all of which are—you guessed it—men. The innovators are deserving of their awards, but to me, the fellas' presence makes women's absence all the more noticeable. You can't convince me that there aren't many women working in IT or that they're not doing noteworthy things. So where are the women in *Windows IT Pro?*

In her blog post "Motivating Women in the SQL Server Community," InstantDoc ID 97176, about the Professional Association for SQL Server (PASS) Women in IT luncheon, Megan Bearly says she "expected at least one of the women on the panel to say that she had to fight to be equal with her male coworkers." But nobody did. And in response to the article "Resources for Women in IT," InstantDoc ID 45462, an anonymous reader says, "We have to read about how women are all upset.... We are developing a society of promoting complaining so media like this can thrive over lack of providing essential material and skills to help improve us all and achieve more within this industry." So maybe I'm just making a mountain out of a *male*-hill. (Sorry, I couldn't resist.)

Tell me: Are women shut off from the IT community, or should I just shut up? Join the discussion at our Women in IT forum at www.windowsitpro.com/go/ITwomen. Or comment on my extended blog post at **www.windowsitpro.com/go/SavvyAssistant.**

Ensuring User Continuity

Companies that implement true high-availability and disaster-recovery solutions to ensure user continuity will, as a result, also protect business continuity. In this Web seminar, learn how to keep users connected and businesses up and running and how to differentiate high-availability and disaster-recovery solutions in the market.

www.windowsitpro.com/go/seminars/neverfail/usercontinuity/?code=citcnov

Consolidation for Optimized Windows File and Print Serving

Learn how clustered storage can "run native" in Windows environments without compromise and deliver scalable file serving with eight times the performance of NAS appliances at a fraction of the cost. Explore possibilities of leveraging existing hardware and see real-world examples of data centers that are reaping the benefits of an industry-standard approach.

www.sqlmag.com/go/seminars/polyserve/consolidation/?partnerref=citcnov

Set the Stage for Exchange 2007

Join Exchange MVP Paul Robichaux in this Web seminar as he investigates the common pitfalls that await you during migration to Exchange 2007, technologies that ease Exchange 2007 migration and administration, and steps you can take to avoid unpleasant surprises. Don't miss this opportunity to ask Exchange experts your toughest questions.

www.windowsitpro.com/go/seminars/NetIQ/MigratingtoExchange2007/?partnerref=citcnov

Quest Wins Again!

Microsoft Global ISV Partner of the Year 2004 and 2007

For Windows management, more people think of Quest Software than any other third-party software vendor. And with good reason. Because when it comes to product quality, customer support and a strong partnership with Microsoft, Quest stands alone. That's why Microsoft chose Quest as their Global ISV Partner of the Year for the second time.

Learn why we are the leader in Windows management.
Visit **www.quest.com/ISVaward**

Microsoft GOLD CERTIFIED Partner

2007 GLOBAL ISV PARTNER OF THE YEAR

QUEST SOFTWARE®

Active Directory | Exchange | SharePoint | SQL Server | .NET | Windows Server | Identity & Access Management

SQL Server 2008: Goodbye, Database; Hello, Data Platform

Microsoft products support Microsoft products

After attending the annual Professional Association of SQL Server (PASS) conference in September and learning about the new features of Microsoft SQL Server 2008, I recalled a July 2006 blog entry by Kevin Kline ("It Depends on How You Define 'Whining,'" InstantDoc ID 53930). Kevin bemoaned the fact that SQL Server has become so complex that even experts can't master all of its vast functionality.

As president of PASS and a columnist for *SQL Server Magazine*, Kevin knows whereof he speaks. And Microsoft has a big job leveraging the strength of that complexity while it's also positioning SQL Server 2008 as a "data platform" rather than simply a database engine. At PASS, I talked with Ted Kummert, Microsoft corporate vice president of the Data and Storage Platform Division, about Microsoft's strategy of positioning SQL Server as a data platform—which, by no coincidence, is similar to how Microsoft Exchange Server is being positioned as a Unified Communications platform and Microsoft Forefront is being positioned as a security platform.

From Database to Data Platform

IT organizations that use Microsoft technologies can't avoid SQL Server even if they want to. Not only are business applications built to access SQL Server databases, but an ever-growing number of Microsoft products—from Windows Server Update Services (WSUS) to System Center, Forefront, and SharePoint—require it on the back end as well. The advantage of SQL Server as a data platform underlying everything is that once you know SQL Server fundamentals, you can apply them in a variety of scenarios.

When I asked Ted about the thinking behind the shift from database to data platform, he said, "What [customers] want is to get some job done, and if they have to learn less to get that job done, that's a good thing for them. We think that's a part of the value proposition of the complete data platform. You deploy it in various workloads: You have it underneath a packaged application; you have it under a custom application; you have it in BI. You have a set of skills and knowledge you can leverage across your organization, and you don't have to have people learn new things just to get the job done."

To enable SQL Server to be this all-encompassing platform, you need the tools to manage the databases, and you need those tools to be as familiar as the database engine. To that end, SQL Server 2008 integrates with the System Center management platform model and embraces the Dynamic Systems Initiative (DSI). (For details about DSI, see "Radically Simplify IT," April 2006, InstantDoc ID 49503, and "System Center Puts DSI into Practice," March 2007, InstantDoc ID 94969, for my interviews with Kirill Tatarinov, Microsoft corporate vice president of the Windows Enterprise Management Division.)

Ted explained, "Fitting in with System Center, we are delivering all the manageability in SQL Server 2008 as part of that framework. We've talked a lot about DSI and that vision. A big part of it is a policy-based administration model for everything in all of our products and infrastructure solutions. We call [SQL Server's] implementation [of policy-based management] the Declarative Management Framework [DMF]. We're very focused on delivering solutions that work well with System Center."

Ted gave an example. "Specifically, you'll be able to see the state of your systems. You'll go to Operations Manager and say, 'These three systems are out of policy,' and it will call DMF to put them back in state."

Another example is the freshly released Microsoft System Center Data Protection Manager 2007 (DPM), which supports SQL Server (plus SharePoint, Exchange, Microsoft Virtual Server 2005, Windows XP, and Windows Vista) and which Microsoft's Jason Buffington demonstrated at PASS. (Jason also explained DPM licensing to me; for details, see the Web-exclusive sidebar "Microsoft System Center Data Protection Manager 2007 Licensing," www.windowsitpro.com, InstantDoc ID 97230.) Being true to the platform model, DPM not only backs up SQL Server, but it also incorporates a free instance of SQL Server 2005 under the covers for reporting.

Why Platforms?

Clearly it's in Microsoft's interest to propagate SQL Server in all of its products: It's hard to switch to a different database and eliminate SQL Server if core technologies such as WSUS require it. But Microsoft sees the idea of its products being "platforms" as a win for its customers, too: The more Microsoft's products to support each other, the less you have to learn when you implement a Microsoft product or version.

I'd like to hear what *you* think. How will Microsoft's platform strategy affect you and your organization?

InstantDoc ID 97229

Karen Forster (karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

Did You Know?

You can download a podcast of Karen Forster interviewing Kirill Tatarinov about DSI at www.windowsitpro.com/go/DSIpodcast.

_INFRASTRUCTURE LOG

_DAY 62: Everyone's completely overwhelmed by their desktops. People keep flipping between browser windows. The in-boxes are overflowing. So many applications. All the user interfaces are different. How is anyone supposed to collaborate when they're flooded with all this stuff? This is so frustrating. We need to get our heads above water.

_Gil has grown gills just so he can stay on e-mail longer. Help.

EDITOR'S NOTE

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

More Mysteries of the AdminSDHolder

Tony Murray's article "Demystifying the AdminSDHolder Object" (June 2007, InstantDoc ID 95834) was excellent. Coincidentally, I read it just a few days before I faced a problem with AdminSDHolder. Tony really saved my day! However, I wish the article had included the workarounds that exist not only to customize the object's behavior but also to disable it. (For more information, see "Delegated permissions are not available and inheritance is automatically disabled," support.microsoft.com/?id=817433.)

—Apostolos Fotakelis

The Microsoft article you refer to provides good supporting information about the AdminSDHolder object, especially for those upgrading domain controllers from Windows 2000 Server. I would, however, urge readers to carefully think through the implications of reverting to Win2K AdminSDHolder behavior as described in the article. The changes to AdminSDHolder behavior were implemented in Windows Server 2003 Active Directory (AD) for a good reason: to improve security. If you encounter the problem described in the Microsoft article, implement the workaround that the article presents as Method 1 rather than the hotfix. This method is the least likely to leave AD open to compromise.

—Tony Murray

64-Bit Recommended

The sidebar "AD Considerations for Exchange 2007" (September 2007, InstantDoc ID 96535) says that "your GC servers must be running a 64-bit Windows OS." This statement isn't true; Microsoft just *recommends* that you use 64-bit Windows. Nice article, though.

—hitchcock4

I pulled this sidebar together from Brien Posey's "Designing Active Directory for Exchange Server 2007" (September 2007, InstantDoc ID 96536). In that article, Brien says that according to Microsoft's recommendation, for the 8:1 ratio of Exchange cores to Global Catalog (GC) cores to be valid, you need a 64-bit Windows OS and you need enough memory to cache the entire AD database in RAM. Sorry for the confusion, and I hope this clears things up a bit.

—Brian Keith Winstead

Licensing Conundrum

Thanks to Nate McAlmond for a great article, "Deploy a Single Application Through Terminal Services" (August 2007, InstantDoc ID 96337). I am deploying a new back-end application and will configure Terminal Services to provide access. I would appreciate some clarification regarding licensing.

In addition to Terminal Services user and device CALs, do I need Windows user CALs for Windows Server 2003, or does the server license cover my licensing obligation? Additionally, my application/Terminal Server will be storing and accessing data from a separate Microsoft SQL Server 2005 machine. Will I be required to buy SQL user and device licenses, or does the SQL Server license cover me?

—Jeffrey B. Mahar

In addition to the server license, you'll need one Windows Server CAL. (See www.microsoft.com/windowsserver2003/howtobuy/licensing/ts2003.mspx for more information on licensing for Terminal Services.) You'll also need a CAL for SQL Server. You can license SQL Server 2005 by user, by device, or by processor. If you license SQL Server by device, you'll also need a CAL for each terminal that accesses the SQL Server machine. However, you could use the processor licensing model for SQL 2005, which would eliminate your obligation for CALs completely.

—Nate McAlmond

Microsoft's Software Plus Services Strategy

I read Karen Forster's IT Pro Perspective column "Microsoft's Software Plus Services Strategy" (September 2007, InstantDoc ID 96673). IT is a very fluid market, and you have to go with the flow to remain competitive. I'd be disappointed in a leader who could not demonstrate agility.

Like any other company, Microsoft is after one thing—profit. It achieves that one thing by way of pervasiveness. Just as it does with its service stack, Microsoft will morph the definition of terms such as service-oriented architecture (SOA) in order to show that its offering is not only complete but also meets the definition and is necessary. Architects have to be wary of any company (e.g., IBM, TIBCO Software, BEA, Sun Microsystems) that does the same thing.

Microsoft is going to do whatever it takes to be pervasive and profitable. It will look at academia and do research, then will use the data gleaned from that research to build its own product map that will foster its mission of profitability and pervasiveness. SaaS is going to have to convince people to let go of their data. More importantly, because of the work that companies such as Microsoft are doing, SaaS will also have to change what we know to be true, which is that "rolling your own" ain't really all that hard or expensive! It will be interesting to see what Microsoft does.

—galaxis13

InstantDoc ID 97320

Oops

In the October 2007 Table of Contents, John Green's "VPN Firewalls for SMBs" was mistakenly printed with InstantDoc ID 95955. To read this October comparative review online, please use InstantDoc ID 97173.

IBM

Take back control of the desktops with IBM Lotus® Notes® and Lotus® Domino® 8.

Control end-user productivity *by putting the applications and tools everyone uses all in one place. An intuitive, Web-like interface means users can work more efficiently and with minimal IT support.*

Control your environment *by easily creating Web 2.0–based composite applications. Your co-workers now have a role-based work space so they can quickly adapt to their changing business needs.*

Control and enhance communications *with integrated e-mail, instant messaging, calendaring, and contact management tools that make collaboration faster and more effective.*

Control your time *with powerful desktop management tools. Now you can centrally manage deployment and upgrades. Open standards give you a flexible platform to easily develop new plug-ins.*

Control your investments *by working with your existing assets and platforms. Backward and forward compatibility means less time and money spent on new apps and on training co-workers to use them.*

Control your overflowing desktops *with IBM Lotus Notes and Domino 8 software, the new standard in desktop and collaboration environments.*

Lotus®

Watch the IBM Lotus Notes & Domino 8 Webcast at:
IBM.COM/**TAKEBACKCONTROL**/LOTUS8

An Amazing Breakthrough in E-Discovery and Recovery.

...FOR EXCHANGE

Makes Complex, Time-Consuming and Expensive E-discovery and Recovery a Thing of the Past.

DISCOVER – DigiScope's robust and flexible search capabilities enable you to rapidly query one or more Exchange databases, PST files, or DigiVault™ data sets to locate a specific mailbox, folder, e-mail item, or entire conversation thread in record time.

RECOVER – Easily restore individual mailboxes, folders, messages, contacts, schedules, and other e-mail items directly to your production Exchange server, or extract the required data into a PST, MSG, XML, or native attachment file format for transport, review, regulatory compliance, or Legal hold.

RELAX – With DigiScope, you can quickly find and recover invaluable lost, deleted, or historical data without implementing never-ending mailbox brick-level backups, costly Exchange recovery infrastructures, or ineffective Recovery Storage Groups.

How it Works

FREE DOWNLOADS

- Demo version of DigiScope
- White Paper –"The Federal Rules of Civil Procedure, E-mail Discovery and You." by Osterman Research

Go to: www.Lucid8.com/Discover
Call: 425 456-8493
E-Mail: Sales@Lucid8.com

Microsoft® GOLD CERTIFIED Partner

Certified for Microsoft® Windows Server™ 2003 Standard Edition Enterprise Edition

Created by Lucid

Solutions Inspiring Confidence

What You Need to Know About ...

Google Apps

For its entire 30-year history, Microsoft has delivered software to users in some physical form, be it a floppy disc, CD-ROM, or DVD. But many customers today are expecting software to be online as well. No company excels at this quite like Google, which provides a host of Web-based applications and services that increasingly compete with Microsoft products and services. Indeed, Google is a company that you should examine in relation to your own needs. Here's what you need to know about Google.

How Google Competes

In addition to its dominant search engine, Google has branched out into a startling array of Web-based products, services, servers, and client applications such as Gmail, Google Calendar, Google Docs & Spreadsheets, Blogger, Picasa, and YouTube. What's particularly amazing is that while Google is somewhat dismissive of Microsoft—Google CEO Eric Schmidt once remarked that the software goliath was "not a significant competitor" online—Microsoft recently categorized Google and other "cloud computing" companies as primary competitors.

So where's the overlap? For the largest enterprise customers, Google is just a distant promise, and the company doesn't offer any of the core infrastructure servers that Microsoft does. For everyone else, however, from individuals to small-to-midsized businesses (SMBs), Google has some compelling solutions.

The most obvious of these is Google Apps (www.google.com/a), a powerful suite of online tools that provide Web-based email, calendaring, IM, Web hosting, and document creation and collaboration (word processing and spreadsheets currently, and databases soon). Individuals and families can use Google's Gmail.com domain or their own domain for free. SMBs and educational institutions can move up to more expansive versions of the service, usually at a very low cost.

The advantages over Microsoft solutions such as Exchange are numerous: Google Apps is hosted and managed by Google, so customers don't need to hire, train, and manage technical staff for services such as email and calendaring. The applications are often less complex than Microsoft's solutions, and since the emerging workforce of recent college graduates is already familiar with Google and Gmail, most don't require much help getting up and running. Google Apps is generally less expensive than Exchange as well, especially for small businesses.

Google has been working to ensure that Google Apps scales to the needs of bigger companies as well, but those needs include such things as security, uptime and performance. It's likely that Google Apps will meet these needs within the next few years, regardless of the size of your organization. Currently, however, the suite doesn't offer the functionality or uptime guarantees most businesses require.

Looking Ahead

One of the most obvious complaints about Web services is that users must be online to take advantage of them. However, two emerging trends make this less of a concern. First, an increasingly large number of users can access Web services from their smart phones, and it's becoming less financially prohibitive for even small businesses to outfit their workforce with such devices. With a smart phone, users are rarely offline, and upcoming changes in rules for air travel will likely eliminate that final hurdle as well.

Second, Google says that it's found a solution for offline Web applications and services. Dubbed Google Gears (gears.google.com), this technology will let users access Google Web services while offline. To date, only one Google service, Google Reader, takes advantage of this technology. Google says that it will bring other services online with Google Gears in the months ahead.

In the meantime, Google is trying to meet customers' offline needs in other ways. As a result of a recent partnership with Sun Microsystems, Google now offers Sun's $70 StarOffice 8 office productivity suite—a competitor to Microsoft Office—for free through the Google Pack service. StarOffice is more like Office 2000 than Office 2007, but it does offer the word processing, spreadsheet, presentation, and database functionality that most customers require, and the price is certainly right. When used in conjunction with StarOffice, Google Apps gives SMBs much of the functionality of Exchange and Microsoft Office—albeit with some incompatibilities—for free or, at worst, for a fraction of the cost of the Microsoft products.

Recommendation

Although Google Apps isn't adequate for most large companies, SMBs should begin to evaluate Google Apps and how it compares with Microsoft technology. Educational institutions especially are an excellent fit for Google's services—though to be fair, Microsoft offers similar if less mature academic packages for its Windows Live Hotmail service.

InstantDoc ID 96986

Paul Thurrott (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Did You Know?

You can read an in-depth review of Google Pack, which includes the StarOffice applications, on the SuperSite for Windows at www.winsupersite.com/reviews/google_pack_2007.asp.

Pro-Active Solutions for User Account Management

Case Study: Chino Valley Unified School District

Advanced Toolware Delivers Real-Time User Life Cycle Solutions for Active Directory

The Situation

The day-to-day management of over 34,000 user accounts was growing increasingly difficult and time-consuming for the Chino (California) Valley Unified School District. The management of all user accounts in Active Directory was an entirely manual process, creating enormous inefficiencies. The district lacked any clear standards and consistency. Third party scripts did nothing to simplify the situation or help with the management of accounts in other applications, such as Renaissance Learning, Riverdeep, Orchard, and Easy Grade Pro.

By June 2006, the system had reached a breaking point. "Because of our constant growth and limited staffing, we had to find a solution that would allow us to streamline and automate our entire user account lifecycle," said Georges Khairallah, Network Specialist for the Chino Valley Unified School District. "That's when we turned to Advanced Toolware."

Out-Of-The-Box Solution

Advanced Toolware immediately identified the key problems within the IT Department and identified four specific requirements:

- Integrate user and directory management with **Aeries CS** Student Information System and other district applications
- Empower users with the ability to administer Active Directory without escalating privileges
- Allow users to perform complex tasks without knowledge of advanced scripting or programming
- Provide transparent auditing and reporting to verify information with the Student Information System

"UMRA's out-of-the-box database connectors saved us valuable time" Georges Khairallah

Next, Advanced Toolware implemented User Management Resource Administrator, their enterprise level software package for Active Directory, to automatically manage user accounts across the domain and securely delegate day-to-day administrative tasks to employees. Automating common operations to run in the background made sense for a district as large as Chino Valley. The ability to integrate the Student Information database with Active Directory and other applications saved countless hours each day. The provisioning process, including account creation with all group memberships and home folders, was also fully automated. As a result, students use the same user name across all applications. The User Management Resource Administrator also ensures that all users are set up correctly the first time and all subsequent updates happen automatically.

Giving faculty and staff the ability to manage users had an immediate impact for the entire district. Teachers can now solve problems with student accounts, without any technical training or administrative privileges. Problems, such as a forgotten password and/or locked out user account, can be quickly solved without involving the IT department. What used to take hours to solve, now takes seconds with the click of a single button.

Instant Return On Investment

Upon implementation, Chino Valley Unified School District immediately realized enormous gains in productivity. The time spent creating accounts each year was reduced from weeks to mere minutes. The process of maintaining student accounts manually was eliminated, saving hundreds of hours annually. Technicians now focus their time and attention on the areas of network management that require their expertise. "User Management Resource Administrator gave us an opportunity to leverage our creativity," said Khairallah. "It opened a big door to creating solutions that we never thought were possible."

Chino Valley Unified School District serves over 33,000 K-12 students. The district is one of the largest in California and has been recognized as the highest ranked school district in San Bernardino County.

Tools4ever Products in partnership with ***Advanced Toolware Consulting Division*** specializes in managing user account information throughout the entire network and offers software solutions to greatly simplify user account management. With thousands of customers worldwide, Tools4ever and Advanced Toolware are committed to delivering superior products and customer support.

For additional information contact Tools4ever at
New York: 1-866-482-4414
Seattle: 1-888-770-4242
Or visit us online at:
www.Tools4ever.com/chino

Use Netsh to Easily Change IP Addresses

In my environment, we don't use DHCP in all locations. In most cases, we use static IP addresses. Using static IP addresses usually doesn't present any problems because we rarely move desktops between locations. However, the people who use laptops usually visit multiple locations. At each location, they've been assigned a separate IP address. Each time they change location, they look up the appropriate network settings in a .txt file, then manually change those settings. This occasionally creates problems because they have to remember the correct steps to change their network settings and sometimes they mistakenly enter wrong numbers.

I recently devised a better solution. For each location, I created a simple batch file that the laptop users can run. Whenever they want to change their IP settings, all they have to do is execute the appropriate batch file.

The batch file uses the Netsh utility and contains only three commands. The first command

```
Netsh interface ip
  set address name="local area
  connection"
  source=static addr=static_ip_
  address
  mask=subnet_mask
  gateway=gateway_ip 1
```

changes the TCP/IP interface. The first parameter sets the interface's name. The name in this parameter needs to match the name specified in the interface's Network Connection Properties page. Although *local area connection* is typically the name for the first interface, it might be different on your laptop, so you should check the properties page. Note that when a name includes embedded spaces, you need to enclose the name in quotes.

The second and third parameters set the location's static IP address and the subnet mask for that IP address, respectively. In these parameters, you need to replace *static_ip_address* and *subnet_mask* with your static IP address and subnet mask.

The last parameter configures the default gateway. You need to replace *gateway_ip* with the IP address of your default gateway. The 1 at the end specifies the metric for the default gateway. Typically, a metric of 1 is configured on all installed network adapters.

The second command in the batch file is

```
netsh interface ip
  set dns name="local
  area connection"
  source=static
  addr=primary_dns_ip
```

This command configures the settings for the primary DNS server, so you need to replace *primary_dns_ip* with the IP address of your primary DNS server.

The last command

```
netsh interface ip
  add dns name="Local
  area connection"
  addr=secondary_
  dns_ip
  index=2
```

sets the secondary DNS server's settings. You need to replace *secondary_dns_ip* with the IP address your secondary DNS server. The index=2 parameter specifies the position of the specified server, which in this case is 2. If you were to add a third DNS server, you'd include this command again—only this time, you'd specify the third DNS server's IP address and change the index number to 3.

Although Netsh has been around for a while (Microsoft started including Netsh in Windows 2000), it isn't the easiest utility to use because it has so many commands and options. You can get help with Netsh by opening cmd.exe and running the command

```
netsh.exe
```

after which you'll get a netsh prompt. If you type a question mark (?) after the prompt, you'll get a list of available commands and how to get syntax information for them. You can also find Netsh documentation in the "Using Netsh" Web page (www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netsh.mspx).

Apostolos Fotakelis

Although Netsh has been around for a while, it isn't the easiest utility to use.

After you create the batch file, you need to give it an appropriate name and place it on the users' desktops. Now whenever the users want to change their IP settings, all they have to do is run the batch file.

Note that users must have the necessary rights to their computer to run the batch file. They don't need to be a local administrator, though. Putting them in their computer's Network Configuration Operators group is adequate. (For more information about this group and its rights, read the Microsoft article "A Description of the Network Configuration Operators Group" at support.microsoft.com/kb/297938).

—Apostolos Fotakelis, Systems Administrator, Aristotle University of Thessaloniki, and freelance IT consultant

InstantDoc ID 97149

EDITOR'S NOTE

Share your Windows discoveries, comments, solutions to problems, and experiences with products and reach out to other *Windows IT Pro* readers (including Microsoft). Email your contributions to r2r@windowsitpro.com. Please include your phone number. We edit submissions for style, grammar, and length. If we print your submission, you'll get $100. Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID number in the InstantDoc ID text box.

The Trick to Accessing Remote Files with Explorer.exe

In his Reader to Reader article "Access Remote Files with iexplore.exe" (InstantDoc ID 95445, June 2007), Serge Bédard mentions that his company's IT staff members have two accounts: a limited-privilege account that they use to log on to their own computers and a high-privilege account that they use to log on to users' computers for maintenance or troubleshooting purposes. Not wanting to constantly use the Net Use command to create a special connection, Serge discovered that he could use the Runas command with Internet Explorer (IE) 6.0 to access to computers under the high-privilege account. He mentioned that he had tried using the Runas command with Windows Explorer (explorer.exe), but it didn't work.

You can use the Runas command with Windows Explorer, but you first need to make a registry edit. Here are the steps to follow:

1. Under the Start menu, select Run and enter the command

```
runas /user:domain\username regedit
```

where *domain\username* is the high-privilege account you want to log on with. Click OK. In the command-shell window that appears, enter the relevant password and press Enter. The registry editor will appear and will be running under the high-privilege account.

2. In the registry editor, navigate to the HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced key. In the SeparateProcess entry, change the value from 0 to 1. I've noticed that this key is missing on some clients. If it's missing, you can safely create the key. Close the registry editor.

3. Under the Start menu, select Run and enter the command

```
runas /user:domain\username explorer.exe
```

where *domain\username* is the high-privilege account you want to log on with. Click OK. In the command-shell window that appears, enter the relevant password and press Enter. Presto—you should have a Windows Explorer window that's running under the high-privilege account. In this window, you can access files on the target remote computers.

If desired, you can place a shortcut to Windows Explorer on your desktop (i.e., the desktop mapped to your limited-privilege user account). To do so, paste a shortcut to C:\%WINDIR%\explorer.exe on your desktop. Right-click the shortcut and click Properties. On the Shortcut tab, click Advanced and select the *Run with different credentials* check box. Click OK twice. Now when you double-click the shortcut, you're presented with the Run As dialog box that lets you run Windows Explorer under the current logon account or a different account. This is where you'd use the high-privilege account.

Simon Drake

Using the Runas command with Windows Explorer is preferable to using the Runas command with IE because, as Serge points out, the Runas command works with IE 6.0 but not IE 7.0. Although I've only used the Runas command with Windows Explorer on Windows XP, this fix will likely work on other OSs as well. If you try this fix on other OSs, be sure to try it on a test machine first. Thanks to Aaron Margosis for his help with creating this fix.

—Simon Drake, Network Administrator, Barnett Waddingham

InstantDoc ID 97150

Hidden Option, Free Utility Can Be Real Time-Savers If You Copy File Paths Often

I regularly need to copy literal paths to files I've found in Windows Explorer. The process of getting a single file path into the clipboard is annoying. You can open a command-shell window and run a command such as

```
Dir /s /b uniquefilename
```

from a directory at least one level above the file to get the whole path in the command-shell window. Alternatively, you can copy the complete address for the open folder from the Address bar in Windows Explorer, paste the address into a text editor, type a backslash (\), go back into Windows Explorer and right-click the filename, select rename, press Ctrl+C to copy the filename, press the Esc key to cancel the rename operation, paste the filename into the text editor to complete the path, and finally select and copy the entire string you've constructed. Even this approach requires customization to be successful; you have to set up Windows so that it shows complete folder paths in the Address bar and shows file extensions for all file types.

Although it's hidden, Windows Vista has a context menu option named Copy as Path that lets you copy a path in a single step. After you select the file, you simply hold down the Shift key while right-clicking. This option works with multiple files and folders as well. When you use the Copy as Path option on more than one item, all the paths are resolved, quoted, and put in the clipboard as multiple lines of a single clip, like this:

"C:\Windows\System32\cluster.exe"
"C:\Windows\System32\cmd.exe"

You don't need to have Vista to easily copy paths from Windows Explorer. Ninotech's free Path Copy utility (home.worldonline.dk/ninotech) works on Windows XP, Windows 2000, Windows NT, and Windows 9x. Path Copy installs an extended context menu item for copying paths. With one or more items selected, you can copy the item's name, path, or parent folder path either as a full path or short path (8.3 format). If you access the item over a network, Path Copy also lets you convert paths to Universal Naming Convention (UNC) format or Internet format (e.g., \\server\Shared%20Files). There's also support for custom modifications, which is handy if you're a scripter or programmer and need to escape backslashes in paths or convert them to forward slashes (/).

Even though I have Vista on my personal PC, I still use Path Copy because I like its flexibility. However, most of my path copying takes place on client PCs, where Path Copy isn't available. As a built-in convenience, Vista's Copy as Path option is turning into a big timesaver for me.

—Alex K. Angelopoulos, Senior Network Engineer

InstantDoc ID 95953

The Essential Guide to

November 2007

Creating an Environment for Sustaining Compliance

By Randy Franklin Smith

Special Advertising Supplement Sponsored by Shavlik

Before the onslaught of today's security-related mandates most companies were already struggling to deal with their own internal mandates for security and control of their IT infrastructure. Now even small companies with a tightly-focused business scope are impacted by multiple security mandates from within the organization, as well as from government, regulatory and industry requirements. Faced with the multiple mandates and looming deadlines it's easy to take a reactive, point-in-time oriented approach.

The challenge of sustainability

In this Essential Guide, I will explain why creating an environment for sustainable compliance is crucial if you are to be compliant and remain compliant—without compliance becoming your organization's very raison d'être. I will discuss the importance of taking a process-oriented approach, how to leverage the commonality between various industry and government mandates, and exploiting technology with an "automate where you can" strategy. Then I will relate these issues to key requirements you should factor into compliance-related purchases so that you reap short-term results and long term value from your compliance efforts.

Multiple Mandates

Today the question is not "Are we subject to any compliance mandates?" Rather, the questions are "How many?" and "How often?" For example, a small publicly-held hospital system finds itself subject to at least two legislative mandates (SOX and HIPAA) as well as one industry mandate (PCI), each with its own deadlines for various tasks, reports and processes. Table 1 lists the legislative and industry mandates most common today.

Mandate	Description
Sarbanes-Oxley Act of 2002	Financial reporting accountability.
Payment Card Industry Data Security Standard	Developed by an alliance of credit card companies to protect payment account data.
Federal Information Security Management Act of 2002	FISMA requires all federal agencies to manage the security of federal information and information systems according to best practices. Specific guidelines are set forth by the NIST.
OMB A-123	This mandate makes federal agencies subject to the same internal controls and financial reporting requirements as those required by public companies under SOX 404.
FCPA - Foreign Corrupt Practices Act	Outlaw companies from bribing foreign government officials for business purposes. Requires controls over transactions and reporting to SEC.
SEC Rules 17a-3 & 17a-4	Requires records related to securities transactions be maintained for 3 years in accessible form.
Basel I/II	Requires comprehensive operational risk management framework for international banking
Health Insurance Portability & Accountability Act (HIPAA)	Confidentiality of patient information
Gramm-Leach-Bliley Act	Banks are required to safeguard privacy of customer financial information
FDA CFR21 Part 11	Security and management of electronic records for clinical trials
DoD 5015.2	Federal records management standards

Table 1 ***Common legislative and industry mandates***

In addition to legislative and industry mandates, many organizations must deal with internally developed security mandates and requirements from business partners (e.g., regular SAS70 audits).

Faced with multiple mandates it's important to recognize the opportunity associated with the commonality between various security mandates. For instance, whether you are complying with SOX, PCI or HIPAA or all three you need to be able to demonstrate good patch management. Identifying such points of commonality is easy. In this example, the challenge is avoiding re-inventing the wheel and eliminating duplicated effort by performing patch management activities once while efficiently producing documentation and reports that satisfy the reporting formats and cycles similar to each mandate.

Compliance mandates are not static nor is the technology and processes they control. For instance, SOX 404 compliance has been impacted several times by revised guidance from PCAOB, Congress and the SEC. PCI has seen revisions. Moreover, new compliance mandates are always around the corner as security threats and disasters push governments and industries to respond to the wide ranging and dynamic threats to information security. Compliance is seldom built into new technologies and little attention is paid. Eventually the technology becomes pervasive and someone realizes important business processes and information subject to compliance mandates are being managed or supported by the technology and once again your compliance environment is impacted. With so much change you can see why it's crucial to architect a change friendly environment if your compliance efforts are to be sustainable.

Compliance is a journey not a destination

Compliance isn't going away. In common across all mandates are initial reporting deadlines and then some combination of ongoing, periodic activities such as quarterly and yearly assessments or reports. The initial deadline of a compliance mandate or remediation of control deficiencies found by auditors and regulators can understandably occupy your waking thoughts. But limiting your efforts to a tactical, fire-fighting approach will leave you with an unsustainable compliance environment.

Under the pressure of deadlines and over-extended resources it's easy to make four crucial mistakes when it comes to your compliance mindset.

1. Taking a point-in-time, project oriented approach

Compliance needs a process-oriented approach instead of strictly project focused mentality, with a perceived ending point. There's no end date for mandates like HIPAA, PCI or others, any more than there is an end date for paying taxes. A "project" attitude impedes long-term compliance efforts and greatly increases associated costs. Employees are pulled from various teams, consultants are hired, and other business and technology projects that could benefit the bottom line are put on hold. As you get past the initial deadlines, employees are left with labor intensive, ad hoc procedures that sap the organization's energy. If you aren't careful, you can be left with a compliant company, but one that has fallen behind in terms of competition or operational efficiency. And when you make a sudden defensive or reactive course correction, other IT projects, business initiatives or processes will likely be impacted without sufficient time to consider the change management considerations.

2. Falling out of compliance

After an organization meets its initial compliance requirements following a project-focused effort, resources are redirected and the staff returns to its "real work." In no time at all the organization has drifted out of compliance. Auditors or regulators point out control deficiencies and a new frenzied project ensues to get back into compliance.

3. Failing to weave compliance into the organization's fabric

Compliance isn't a discreet task that you can simply assign to a department or outsource. Compliance mandates impact processes across the entire organization and any organization that fails to admit this will find themselves embroiled in a non-compliance crisis sooner or later. You need to embrace compliance mandates rather than disdainfully deal with compliance at arm's length.

4. Missing out on the business value of compliance

As much of a nuisance as security mandates and their associated reporting may seem they are, after all, based on proven best practices. The challenge faced by teachers presents an interesting analogy. More and more teachers are evaluated based on how well their students perform on standardized tests. Such a teacher must choose between preparing his or her students for taking a specific exam or they can teach them the knowledge and skills the exam is intended to test. Organizations have a similar choice. They can take a "follow the letter of the law" approach where all compliance efforts are based on passing audits and producing acceptable reports. Or the organization can focus on implementing the actual controls and processes lead to a business passing audits on merit rather than fancy documentation. Businesses that choose the latter will reap the business value, risk mitigation and

operational efficiencies associated with following best practices.

Compliance is an ongoing fact of life and compliance efforts must incorporate a process-based approach. Focusing on deadlines leads to improvisation. Quick, short-term fixes for compliance lead to redundant processes and technologies that increase costs and drag down efficiency while important business initiatives stagnate. Therefore, organizations that implement well-designed, repeatable processes will build a sustainable compliance environment. Moreover, a company that embraces compliance as a business driver for implementing best practices will gain the financial and security benefits that result from such best practices.

Technology Issues

Technology comes into play in two key ways in compliance. First, to meet security mandates the organization's existing IT framework becomes the subject of many activities—including assessments, remediation, reporting and monitoring. Much of the work associated with these activities is onerous and labor-intensive, which brings up the second role technology plays in compliance.

Security mandates have created the need for technology solutions to support the new required activities of documentation, assessments, monitoring, and reporting. There is great potential for automating much of the laborious, almost mindless work associated with these activities. Not only can automation free up skilled IT professionals from performing onerous manual tasks, automation can also improve the effectiveness of controls.

Take log management as an example. Collection, monitoring and archival of security logs is directly or indirectly a requirement of most security mandates. For instance, PCI Requirement 10 mandates that you "Track and monitor all access to network resources and cardholder data)" and includes sub-requirements that specifically address log management. But when you consider how many systems and devices generate security logs and the vast amounts of data generated every day by such systems—as well as the arcane format and content of security logs—it quickly becomes evident that this is not a job for humans. Instead, the business must invest in a log management solution that automates these activities and produces informative reports and alerts, which can then be acted on by busy IT professionals.

Not all compliance activities can be automated. Judgment-call decisions and complex analysis requires a skilled human. Freeing up staff for the tasks that really demand their abilities is crucial to improving efficiency, reducing compliance costs, complying with the spirit of the law and getting business value out of compliance efforts. Freeing up staff requires careful investment in compliance technology solutions that automate what can be automated and that give staff the information they need.

Leveraging technology to build a sustainable compliance environment

Creating a sustainable compliance environment requires that an organization embrace security mandates with a process-oriented, "compliance is here to stay" approach and implement technology solutions that fit into and facilitate this approach. In this section, I will discuss the key requirements for solutions that help build a sustainable compliance environment.

> **Creating a sustainable compliance environment requires that you embrace a "compliance is here to stay" approach.**

Support multiple mandates

Because organizations are subject to multiple security mandates, your compliance solutions should support multiple mandates as well. The solution needs to be open and flexible to handle multiple internal and external mandates.

For instance, consider a medium size company with 1000 employees that is subject to PCI and SOX. For PCI, they must prepare for quarterly internal PCI audits and one formal external PCI audit per year. To comply with SOX, they also must prepare for one internal SOX audit and one formal external SOX audit per year. That adds up to preparation and production of deliverables for seven audits within the framework of two different mandates each year. Their solution needs to seamlessly address their internal and external needs.
Therefore, the ability to address multiple mandates is vital. It's great if the solution enables an organization to assess compliance with SOX – if SOX is the only

mandate with which the organization must comply. But if the solution doesn't handle multiple mandates easily, how is it helpful to a customer who has to comply with their internal mandates, PCI and other legislative or industry mandates?

Of course, this becomes even more of an issue as new mandates come along. Ideally, the ability to demonstrate compliance with future mandates shouldn't require a bolt-on component or a new solution. Well architected, extensible solutions should allow you to pull in new frameworks or templates easily.

Facilitate continuous processes

As this guide has shown, sustainable compliance requires a long-term view that treats compliance as an ongoing process rather than a project with a clear end date. While project tracking and management tools have a place in compliance, investment in tools that penetrate the very core of the compliance problem yield more return on investment over the long haul.

Automate where you can

IT systems and devices were never designed with compliance with security mandates in mind. Therefore, much of the work associated with compliance is backbreaking, onerous labor. The ability to automate assessment, remediation, and maintaining compliance with specified mandates is critical to demonstrating the value of compliance technologies. If you devote an army of IT administrators to these activities labor intensive your costs will increase and the value derived from resources spent on compliance will diminish. Automate what you can. It is unlikely you can automate every requirement in any of the mandates, but automate the pieces you can so you can put your best and brightest staff on things you cannot automate–analysis and decisions that leverage their skills and abilities.

Initial implementation effort

Although I've focused on the long-term, continuous reality of compliance, I should note that the short-term still matters when looking at compliance solutions. A complex, difficult solution won't get fully implemented; the effort will stall without bringing you closer to initial compliance–much less sustained compliance. Many external mandates (i.e., PCI and FDCC) have deadlines looming for compliance. A solution that takes six months to implement means it will be six months before you can demonstrate compliance. Solutions that take hours to install help jump start your compliance effort.

Built-in intelligence

The most overlooked component of a good compliance solution is the ability to automatically generate meaningful reports that not only help manage systems but that also demonstrate compliance with multiple internal and external mandates.

Compliance activities such as risk assessment, auditing and monitoring require quick analysis of vast amounts of data. It's easy to write a program that collects a glut of data, does a little reformatting and simply throws it back out to the unfortunate IT professional who is left to define and generate meaningful reports out of that mountain of detail. If the solution cannot produce informative, actionable reports, how useful is it? If your army of IT administrators is tied up manually creating color charts and graphs in Excel, they aren't focused on the portions of compliance that cannot be automated and need their skills.

An effective solution allows you to gather data (assess), reconcile that data against your security policies, correct (remediate) or manage exceptions across your environment. Then the solution should reuse the data built from those activities to report the findings in the context of multiple security mandates. For instance you should be able to create compliance reports for PCI, HIPAA, SOX that are based on the same assessment and remediation efforts.

Conclusion

You should be able to leverage your investment in compliance related tools to demonstrate compliance with multiple mandates without repeatedly re-inventing the wheel. Additionally, compliance is not a single, point-in-time project. Mandates change. Systems change. Businesses change. New mandates are created. To keep up you need an easy-to-use, cost-effective method to identify and remediate weaknesses and periodically generate reports that demonstrate compliance in an ever changing environment. And, when the next mandate comes along, you can't afford to re-architect your entire compliance strategy. These are the reasons why it is important to implement a compliance solution that takes a holistic approach to compliance, that supports all the mandates to which you are subject and uses a process oriented method to facilitate sustainable compliance.

In the final analysis, compliance solutions provide an important way to reduce costs, while improving compliance and helping realize business value from compliance efforts. The solution should help you 1) improve your security posture, 2) ensure that in making your organization more secure your also comply with multiple mandates such as PCI and SOX, and 3) generate reports about your security posture that link back to internal and external mandates, demonstrating you are in compliance.

Randy Franklin Smith is a contributing editor for *Windows IT Pro*, an information security consultant, and CEO of Monterey Technology Group. He teaches Monterey Technology Group's Ultimate Windows Security course series and is an SSCP, a CISA, and a Security MVP. He can be reached at www.UltimateWindowsSecurity.com.

Simplifying Security and Compliance:

The cost of compliance continues to grow as customers must continually assess and compare their system configurations and policies against both internal and external mandates, and then provide proof of compliance several times a year.

Shavlik NetChk® Compliance reduces risk and increases operational efficiencies for our customers by automating the steps required to develop secure configuration policies, ensure systems remain in policy, and then easily generate operational and executive level reports to prove system compliance with policy. Shavlik NetChk Compliance provides our customers with the most direct route to sustainable compliance, providing immediate results instead of the months-long IT project that many competitive solutions require.

Why choose Shavlik NetChk® Compliance?

- **Change Management –** Enabling appropriate change management controls reduces the risks associated with unauthorized changes such as downtime due to system failure, introduction of security vulnerabilities, and insider security threats. Shavlik NetChk Compliance manages the data related to policy and configuration changes and provides reporting and review of these changes to help customers address IT and regulatory agency requirements for auditing, managing and maintaining security.
- **Configuration Policy Management –** Provides a comprehensive method of detecting systems that have drifted out of compliance with corporate policy, and then quickly remediate or enforce the existing policies, returning the affected systems to the "desired state." This capability helps to reduce risk by driving greater efficiency into the configuration management process.
- **Audit-Ready Reporting –** Allows the user to easily create a variety of "audit ready" reports which demonstrate that the proper configuration controls are in place and operational. These reports can also provide alignment between the various regulations (SOX, HIPAA, etc.), with the requirements of either internal or external auditors who utilize industry standard policy frameworks to measure compliance and prove "due care" has been taken.
- **Policy Cloning & Distribution –** Offers advanced "Gold Machine" scanning automation that helps save time by streamlining the creation of security configuration policies by leveraging existing, approved system configurations. This automation makes it very easy to create a security IT infrastructure that can be measured against a pre-defined industry standard baseline.
- **Policy Mapping and Regulatory Audit –** Addresses current regulations like SOX, GLBA, HIPAA and FISMA that place new demands on information security. Audit systems using the links between best practices content and auditing standards such as ISO 17799 and NIST 800-53. Use these standards to develop powerful security standards to drive an overall security policy.

Simply Create New Charts/Graphs & Customized Views – Allows users to drill down into the real data driving the real-time dashboard reports.

Shavlik NetChk® Compliance provides a powerful engine to scan for, compare, and enforce security settings on your systems.

EDITOR'S NOTE: Send new product announcements to products@windowsitpro.com.

Identity Management

Manage Microsoft ILM 2007

MissionControl 2.2, NetPro's management product for Microsoft Identity Lifecycle Manager (ILM), is now fully compatible with ILM 2007. New capabilities include trending views and details on key data and statistics, 24 × 7 health monitoring, change auditing, and backup and restore. For more information, contact NetPro at 602-346-3600 or visit www.netpro.com.

—Barb Gibbens

Security

Fortify Branch Offices Against Multiple Threats

Fortinet introduced **FortiGate-60B** and **FortiWifi-60B** security appliances for enterprise branch offices, retail outlets, and small businesses. The appliances have an application-specific integrated circuit to accelerate performance, a front-accessible third-generation PC Card slot, dual WAN interfaces, an integrated analog modem, six internal interfaces, and one demilitarized zone interface. The FortiWifi-60B adds 802.11 a/b/g support. Both appliances offer firewall, antivirus, VPN, intrusion prevention system, antispam, Web content filtering, and traffic shaping functions and are updated by the FortiGuard subscription service. For more information, visit www.fortinet.com.

—Renee Munshi

Messaging

View Document Revisions Securely via OWA

Messageware announced that the latest version of its Outlook Web Access (OWA) add-on, **AttachView 8.5**, supports Microsoft Word's Track Changes feature. Users accessing documents via OWA can view them as secure Web pages that display Word revisions and related information, such as revision date. By converting attachments into HTML pages, AttachMate closes a security loophole in OWA by preventing attachments from being stored in shared computers' Temporary Internet Files, where other users could access them. For more information, contact Messageware at 905-812-0638 or visit messageware.com.

—Anne Grubb

Storage

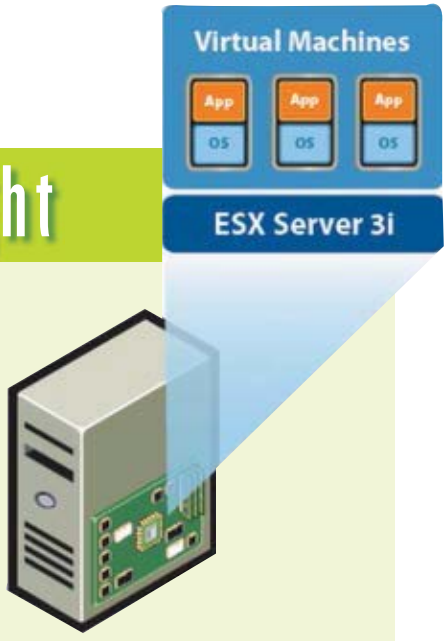
Enhanced iSCSI Connectivity

ATTO Technology is releasing firmware version 4.0 for its **iPBridge** product line, which provides a solution for adding iSCSI connectivity to SCSI and Fibre Channel storage. New features include an ExpressWizard that automatically configures the bridge to operate as efficiently as possible in the specified environment; an ExpressFairness feature (only on the iPBridge 2700) that optimizes data transfers when many hosts are connected to the iPBridge; and a redesigned GUI for accessing the firmware, utilities, manuals, and drivers on the product CD-ROMs. For more information, contact ATTO Technology at 716-691-1999 or visit www.attotech.com.

—Lavon Peters

InstantDoc ID 97024

Product Spotlight



Server Virtualization

Virtualization Hypervisor Embedded with Server Hardware

VMware has announced **ESX Server 3i**, the first hardware-integrated virtualization hypervisor. According to VMware, this new version of the ESX Server architecture is designed to be integrated into flash memory on server hardware, allowing customers to run a functional hypervisor right out of the box.

Because ESX Server 3i will not incorporate or rely on a general-purpose OS, VMware claims that it eliminates many of the common security and reliability problems that arise with running virtual machines (VMs) on top of an OS. Since it is contained in flash memory on the server, ESX Server 3i eliminates installation steps and relies on a Common Information Model to monitor hardware resources. An integrated command-line interface can be used for system configuration, performing maintenance, and installing patches. According to VMware, the automatic configuration features of ESX Server 3i can streamline the setup of VMs and minimize management overhead.

Hardware manufacturers are scheduled to begin shipping server hardware with integrated ESX Server 3i technology by the end of 2007 and throughout 2008. For more information, contact VMware at 877-486-9273 or visit www.vmware.com.

—Jeff James

NEW RELEASE

"This is by far the best defrag product… After installing Diskeeper 2008 I don't have to worry about disk fragmentation ever again. It does everything for me invisibly in the background."

Jozo Capkun, *President*
Komoko Services Limited

It's Smart.
It's Transparent.
It Will Take Your System From Zero to Sixty—*Automatically!*

Automatically and invisibly solve disk performance issues—forever

File fragmentation—the splitting of files in tens, hundreds or thousands of pieces—puts the brakes on system performance. It slows access to a crawl. It causes delayed application launches and slow boot ups. It can even cause system crashes.

Introducing the first and only completely automatic defragmentation solution. New Diskeeper® 2008 with InvisiTasking™ defragments in real-time, invisibly in the background. Intelligently monitors and utilizes only idle system resources, while users continue to work. And with fragmentation completely eliminated, your performance flies. Systems are maintained at peak performance and reliability—*automatically!*

- ***True transparent, background defragmentation,*** *unnoticeable to applications and users—except, of course, for the newfound performance and reliability.*
- ***No scheduling required.*** *Ever. Ever. Ever.*
- ***Adaptive technology boosts access*** *to your most commonly-requested files, beyond defragmentation alone.*
- ***Work smarter not harder.*** *Each volume is different. Dynamic intelligence determines and delivers maximum minute-to-minute benefits with minimal effort.*
- ***Advanced defragmentation*** *uniquely designed for high-capacity, high traffic disks.*
- ***No room to move? Extreme fragmentation? No problem.*** *New, complete defragmentation in all conditions—even with less than 1% free space.*
- ***Critical system file fragmentation*** *now automatically prevented.*
- ***Allows you to leverage VSS data protection*** *and the performance and reliability of defragmentation.*

FREE OFFER

NEW *with InvisiTasking™*
Diskeeper® 2008
Maximizing Performance and Reliability—*Automatically™*

Try New Diskeeper 2008 Free for 45 Days!

Download at www.diskeeper.com/win2008

Note: Special 45-day trialware is only available at the above link

Volume licensing, government and educational discounts are available from your favorite reseller. For a free quote visit www.diskeeper.com/quote10 or call 800-829-6468. *Code 4006*

Diskeeper corporation

Insights from the industry

VMworld 2007: Kace, Pano Logic, and Microsoft

If any attendees of VMworld 2007 still had doubts about virtualization being a vital and rapidly growing part of the IT infrastructure, those doubts were likely erased by the sheer size and scope of the show, which was held in San Francisco in September. According to VMware, more than 10,000 attendees descended on the Moscone Center for this year's event, compared with 7,000 last year. Even the number of exhibitors and sponsors increased, jumping from 82 to 147.

Windows IT Pro Technical Director Michael Otey and I attended VMworld this year, and we found product vendors and IT pros alike taking advantage of the benefits that virtualization offers.

In a morning meeting with the folks at Kace, a provider of systems management appliances, I learned that the company recently announced that its Kace appliance now manages both virtual and physical client machines. During the demo, I found two features of the Kace system notable. The first was a drag-and-drop provisioning feature that lets IT pros simply click and drag colored boxes, representing remote software installs, into a software distribution package. The second was a full-featured script editor that lets nonprogrammers create powerful scripts using a mouse-driven interface.

Kace CTO and President Marty Kacin came up with one of the most notable quotes of the day when he described the Kace system as a "jukebox for digital assets in the enterprise." Kace has other news related to virtualization coming down the road, but I've been sworn to secrecy until Kace is ready to release the news officially.

Microsoft's modest VMworld presence was dwarfed by VMware's sprawling booth.

Pano Logic's Pano device: The ultimate thin client?

I then met with Pano Logic, a startup that's developed the ultimate thin client. The Pano device is a gleaming cube that houses all the ports and connectors for local peripherals but has no RAM, CPU, or local storage whatsoever. Clients run off virtualized desktop software that sits on a virtual machine in the data center.

Vice President of Product Management Michael Fodor explained that the Pano was made possible by several recent developments, ranging from the increasing reliability and predictability of enterprise networks to the advent and adoption of virtualization in the data center. Because the Pano draws only about 3 watts, compared with 15 watts for other thin clients and 150–300 watts for PCs, it can even help enterprises lower energy costs.

Although VMworld spotlights VMware, Microsoft made an appearance at the event. Michael and I chatted with Larry Orecklin (general manager, System Center Marketing) and Mike Neil (general manager, Virtualization) about the latest from Microsoft in the virtualization space. In early September, Microsoft released System Center Virtual Machine Manager, which will be upgraded in the future to manage not only virtualized environments based on Windows Server 2008 (formerly code-named Longhorn) and Windows Server Virtualization, but also Xen and VMware virtualization formats. Orecklin explained that this development would make it easier for customers to integrate their existing physical and virtualized assets.

In addition to a modest booth at the show (which was dwarfed by VMware's massive presence), Microsoft had a single meeting room stuck back in a corner on one of the show floors, next to the exit and maintenance equipment. Granted, this show is primarily about VMware and its partners, but I have to think that Microsoft isn't accustomed to occupying booth space in the trade-show equivalent of nosebleed seats at Yankee Stadium.

—Jeff James

InstantDoc ID 97049

THREE GREAT REVIEWS FOR

THE BOMGAR BOX™

"one of the best help-desk support solutions examined by the CRN Test Center"

CRN TEST CENTER RECOMMENDED ★★★★★ 5 STARS

June 21, 2007
Bomgar B300™
Version 9.3

"a direct link into problem Windows and Mac machines"

NETWORKWORLD CLEAR CHOICE
4.65 OUT OF 5

January 8, 2007
Bomgar B200™
Version 9.1

"a cost effective, secure, elegant hardware solution for remote customer support"

PC MAGAZINE www.pcmag.com ●●●●○ 4 Stars

May 7, 2007
Bomgar B100™
Version 9.2

TEST DRIVE BOMGAR TODAY 866.205.3648 | WWW.BOMGAR.COM/ITPRO

BOMGAR™

The Box That's Revolutionizing Remote Support™

Paul's Picks

Summaries of in-depth product reviews on Paul Thurrott's SuperSite for Windows

www.winsupersite.com

Google Pack with Sun StarOffice

PROS: A free, full-featured office suite, selective application installation.

CONS: Few applications are sophisticated or enterprise-friendly.

RATING: ◆◆◆◇◇

RECOMMENDATION: Google Pack is a free, consumer-oriented collection of software provided by or recommended by Google, and would normally only interest the smallest businesses. That changed somewhat when Google included the **Sun Microsystems StarOffice** suite—a product that normally costs almost $100 per desktop—for free with Google Pack. The suite can't compare to Microsoft Office 2007, but it's still quite capable and is a viable alternative to older versions of Office.

CONTACT: Google • 650-930-3555 • www.google.com

DISCUSSION: www.winsupersite.com/reviews/google_pack_2007.asp

Windows Vista SPI Beta

PROS: Aggregates previous fixes, improves Vista's stability and performance.

CONS: No major new features, no slipstreaming.

RATING: ◆◆◆◆◇

RECOMMENDATION: Microsoft has finally unveiled the feature set for Vista SPI and made the code available in limited beta form. The SPI beta supports Microsoft's view that businesses gain no advantage by waiting on SPI to deploy Vista: It includes no major new features or functional changes and doesn't dramatically alter the Vista experience. Instead, Vista SPI is a service pack, aggregating previously released fixes into a single installer. Microsoft's plan to provide drag and drop slipstreaming with Vista isn't included in this release.

CONTACT: Microsoft • 800-426-9400 • www.microsoft.com

DISCUSSION: www.winsupersite.com/showcase/winvista_spI.asp

InstantDoc ID 97017

Radmin 3.0

Editor's Note: This is a summary of John Green's review of Radmin 3.0. To read the complete article, go to www.windowsitpro.com and enter 97125 in the InstantDoc ID box at the top of the page.

Famatech's **Radmin 3.0** remote-control utility consists of two components: Radmin Server, which supports connection to and remote control of the Windows system you install it on, and Radmin Viewer, which lets you connect to systems running Radmin Server. Both components install quickly and easily, and Famatech supports remote installation via Group Policy. Radmin Server parameters are stored in the registry, so you can save and customize a Windows Radmin uses 256-bit Advanced Encryption Standard to secure all transmissions. You can choose Active Directory (AD)–based authentication or Radmin's user-based authentication, which employs 2,048-bit Diffie-Hellman key exchange. An icon in the system tray offers access to Radmin Server's settings window but appears only when the logged-on user is a local or domain administrator.

In all respects, including drag-and-drop, right-click, and scroll-wheel operations, using the mouse and keyboard worked on the remote computer just as if I were sitting at it.

In all respects, including drag-and-drop, right-click, and scroll-wheel operations, using the mouse and keyboard worked on the remote computer just as if I were sitting at it. Radmin's flexible display support offers Normal, Full Screen, Stretch, and Full Screen Stretch modes. The product also conveniently supports both text and voice chat between users of Radmin Viewer and Radmin Server.

Radmin does have some limitations. Although Radmin Viewer happily operates in the x64 environment, Radmin Server lacks support for x64 versions of Windows. (That feature is in development, with availability expected around the end of 2007.) Also, Radmin Viewer doesn't display the screen contents of remote systems that are operating with a command prompt window in full-screen mode.

With the improved version of Windows Remote Desktop that Microsoft distributes with Windows XP SP2, why would you want to spring for Radmin? For several reasons. Radmin is simply much more pleasant to use than is Remote Desktop, and its File Transfer window is always available for copying a file in either direction. The ability to organize remote computers in a tree hierarchy is convenient, and the multiple-viewer feature is great for consulting with another technician. If you're responsible for user assistance or for server applications that don't have remote console support, Radmin will make your life easier.

—John Green

InstantDoc ID 97125

SUMMARY

Radmin 3.0

PROS: Intuitive interface; multiple independent connection modes support view-only connection and voice and text chat; encrypted communications; AD and Radmin user–based authentication options

CONS: Doesn't support 64-bit Windows OSs

RATING: ◆◆◆◆◆

PRICE: $49 per controlled system; quantity discounts available

RECOMMENDATION: This is the best remote-control product I've tested, and I recommend it without reservation.

CONTACT: Famatech • 877-723-6467 • www.radmin.com

BioPassword Enterprise Edition 3.2

Flexible, effective, software-only 2-factor authentication

BioPassword Enterprise Edition 3.2 (BPE) enhances the security of corporate networks by adding a second, biometric component to the standard Windows logon / authentication sequence. As a software-only solution, it does so without the need for the additional client hardware required by other modes of biometric authentication such as fingerprint identification or retinal scanning. Instead, BPE relies upon the consistent, distinctive pattern of each person's keyboard keystrokes during the logon process.

BPE's streamlined design will appeal to small organizations, and its support for a variety of environments lets it integrate easily into large enterprises. Supported environments include Citrix and RDP / Terminal Server users; selected thin clients with embedded Windows XP; and integration with Microsoft Outlook Web Services. Web application support allows you to integrate BPE into your own forms-based authentication screens.

BPE improves the standard Windows authentication sequence by extending the Active Directory (AD) schema within the AD domain tree hosting user IDs, and by inserting BPE GINA (Graphical Identification and Authentication) stub modules into the domain's GINA chain. This requires that you install BPE on all domains that host either User or Computer accounts that will participate in BPE's two-factor authentication. BPE is active during the primary AD login sequence and will optionally run during secondary logon sequences, such as Run As, Connect As, and Net Use.

BPE works by using client software to record keystroke timings as users complete the User ID and Password fields of an authentication form. Keystroke timings include the dwell (how long a key is held down) and flight (the time between key strokes) times. Using the timings, the authenticating domain controller (DC) calculates a Security Level score. That score is compared to a template created when the user first entered the user ID and password combination. To enroll, a user keys the user ID and password several times until BPE identifies the user's consistent pattern. In my testing, this required eight or more repetitions. As administrator, you may configure enrollment to complete at the user's first logon attempt, or gradually (and transparently to the user) over successive logon attempts.

The implementation process has many steps, but is fairly straightforward. Basic AD installation updates the AD schema, then installs software on all PDC emulators in the tree, on all authenticating DC's, and on all client computers. Other supported environments require additional installation steps. BPE isn't enabled upon installation, and it won't participate in the authentication process until you enable it both for the participating domains and for the participating user IDs.

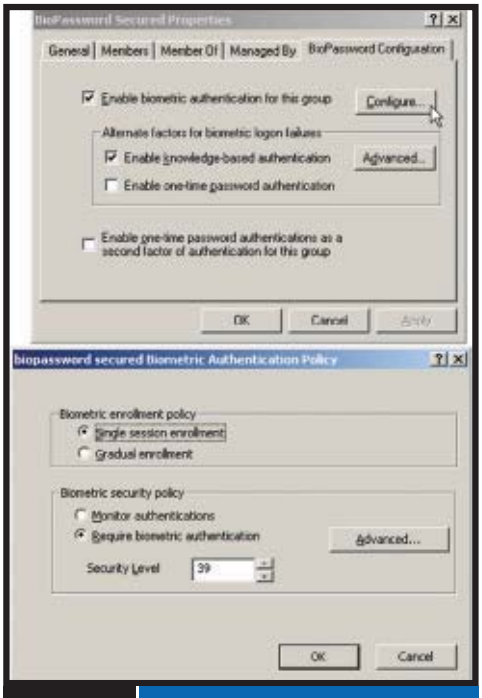


Figure 1: Enabling BioPassword authentication and required security levels

To test BPE, I installed it to a domain with a single DC. I installed the client component to several computers that were members of that domain and to a computer that was joined to a trusted domain and enabled BPE authentication for them. You can enable user accounts for BPE either individually or by enabling a group they belong to for BPE authentication. Figure 1 shows the BPE properties panels used to enable and configure BPE for a group. Finally, I enabled BPE for the domain.

BPE caused me to pay close attention to the logon process, as BPE requires a continuous flow of keystrokes. I enlisted several other regular users of computers in the testing, to see if the "wrong" user could successfully authenticate. This occurred only once in the course of my testing. Administrators can determine how stringent or relaxed their authentication environment will be by requiring a higher or lower BPE security level score.

I found BPE to be effective and relatively easy to work with. BPE provides an evaluation kit to facilitate testing and configuration. Many people will find that installing BPE isn't a trivial process in their environments, but the added level of security will make it all worthwhile for many of you. The implementation flexibility that BioPassword has designed into the product will help ease that effort, and the support for several popular ways users access their applications makes this a viable product for many enterprises. For those seeking to add multifactor authentication as a way to increase system security, I recommend that you take a look at BPE.

—John Green

InstantDoc ID 97102

SUMMARY

BioPassword Enterprise Edition 3.2

PROS: Effective two-factor authentication without the need for special hardware; support for many application access modes, including Citrix, RDP and embedded XP terminals

CONS: Requires an AD schema update; installation is not trivial for large enterprises

RATING: ◆◆◆◆◆

PRICE: $50/user perpetual license + maintenance or $19/user annual subscription, with volume discounts.

RECOMMENDATION: BioPassword is an impressive product, with a lot of implementation flexibility. I heartily recommend it to those seeking to implement multifactor authentication.

CONTACT: BioPassword, Inc. • www.biopassword.com • 425-649-1100

3 TOOLS TO MANAGE GROUP POLICY

by Eric B. Rux

These products vary in approach, but all function well when change management is integral to the environment

Microsoft is good at giving systems administrators cool product features that make our lives easier. Take Group Policy, for example. What started as simple (yet problematic) Windows NT 4.0 System Policies has turned into an enterprise solution for managing desktop settings and deploying software. You can use Group Policy to do things like remove the Run command from the Start menu (to help prevent users from gaining a command prompt), display a logon message that users must acknowledge before logging on, and run scripts for logon, logoff, and even start-up and shut-down. If a policy isn't available to do something you want, you can very often create your own by using an Administrative (.adm) template. If you're not using Group Policy in your infrastructure, you're missing out on one of Active Directory's (AD's) most important features.

But unfortunately, for large environments, Microsoft doesn't always provide the best tools to manage Group Policy. Group Policy Management Console (GPMC) was released in 2003 and was a great improvement over the original tools that came with the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in. But GPMC lacks robust features for a complex AD environment, such as change-management capability, an offline repository, and version control. Here's where the products in this review enter the picture. **NetIQ Group Policy Administrator**, **NetPro GPOADmin**, and **ScriptLogic Active Administrator** all seek to fill voids in the Microsoft tools. The products take varying approaches to Group Policy management, but they all give administrators tools to keep track of Group Policy in an environment that requires change management.

Two products that fit the criteria for this comparative review are missing from it. Quest Software, which recently purchased ScriptLogic, requested that we include ScriptLogic Active Administrator here, rather than Quest's Group Policy Manager. And Microsoft's recent acquisition of DesktopStandard has resulted in the former DesktopStandard product GPOVault being unavailable for review at this time.

The Testing Environment

To test the products, I used VMware Server 1.0.3 to set up a simple AD domain. Each domain controller (DC) was a Windows 2003 Server machine running SP1 with up-to-date security patches. I used each product to edit existing policies as well as to create new ones.

In addition, I ran each product through a typical change-management scenario that might be found in a structured IT department. Specifically, I altered the password requirements in a default domain policy. Unlike a small shop, where one or two administrators can freely make changes at will, a large, structured, enterprise IT department will demand a formal process whenever network settings are changed. I've worked in both situations, and I learned that, at first, change management can seem stifling and unnecessary. However, you quickly come to understand that the processes are in place not only to protect the network but also to protect *you*. Imagine the consequences of changing password policy without proper approval in an enterprise environment.

So, based on my experience, I created the following typical Group Policy change-management process, then I used each of the products I reviewed to implement Group Policy within the process:

1. A request is made to create or alter Group Policy.
2. The request is reviewed by peers and tested in a lab.
3. Implementation is approved.
4. The original Group Policy Object (GPO) (if applicable) is backed up for rollback purposes.
5. An offline GPO is created, edited, then verified by peers.
6. The approved GPO is linked to the appropriate organizational unit (OU), and the old GPO is unlinked, if applicable.
7. Verification that the new GPO is in production is made.
8. Changes made to GPOs are audited periodically to ensure that the rules are being followed.

In addition to observing how each product fit into a change-management process, I looked at how easy it was to work with the product. Did the installation make sense? Was the interface intuitive and easy to navigate? And, were there any compelling features that set one product apart from the others?

NetIQ Group Policy Administrator

I had a lot of trouble installing NetIQ's Group Policy Administrator, but not because there was a problem with the NetIQ product. Rather, the instructions for installing the application were incorrect. The "Trial Guide" clearly states that you can use Microsoft Data Engine (MSDE) to store the Group Policy Repository (Group Policy Administrator's offline version of your GPOs), which Figure 1 shows. I read and reread the Trial Guide (i.e., *Group Policy Administrator Trial Guide.pdf*) but couldn't get the product to install. I eventually called NetIQ technical support and learned that the Trial Guide was a rewrite (dated February 10, 2006) of the earlier 4.0 product version, that some important information has been left out, and that this is a known issue at NetIQ. I expressed to the technician my opinion that a Trial Guide with known misinformation from 2006 should have been updated by now. I was told that it would be updated when the next version of the software comes out. The technician was friendly and extremely knowledgeable about the product. I just wish the Trial Guide had been correct so that I hadn't had to call him in the first place. If you decide to give Group Policy Administrator a try, be sure to review the hardware, software, and network requirements for NetIQ Group Policy Administrator 5.0 at www.netiq.com/support. Look for Knowledge Base article 70246. In the end, I had to install Microsoft SQL Server 2000 SP3 to evaluate Group Policy Administrator.

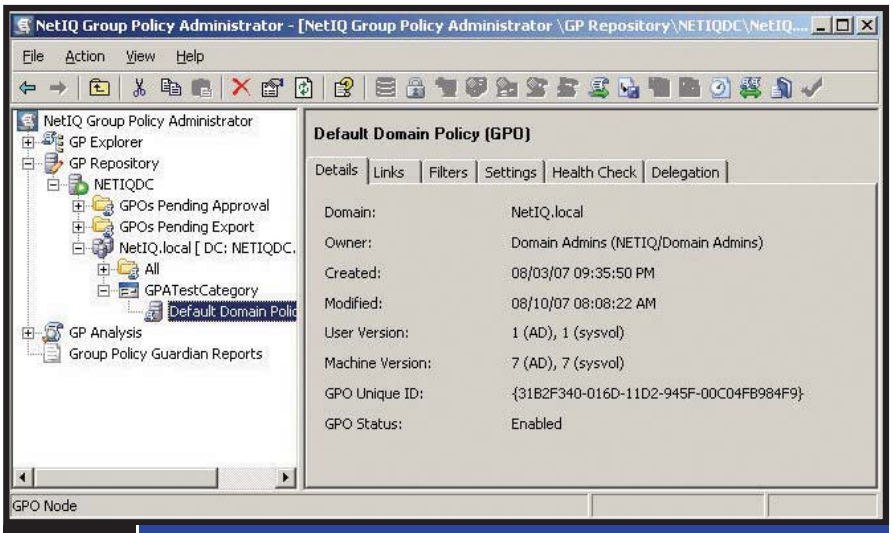


Figure 1: Group Policy Administrator's GP Repository

Testing Group Policy Administrator

The Group Policy Administrator Roles and Delegation wizard lets you specify who can create, edit, and link GPOs (as well as many other permissions) from within the GP Repository. You can designate a Group or User, what kind of permissions they will have, and which repository or specific Group Policy within the repository the permissions apply to. Keeping a tight leash on the repository will help prevent it from becoming a mess of half-used and obsolete GPOs.

To change the password policy within the change-management process I described earlier, I first located the default domain policy and backed it up by right-clicking the GPO under the GP Explorer node in the administrative interface and choosing Backup. Group Policy Administrator stores backups as regular folders, so you need to save them on a file server that's backed up regularly. If you need to restore a GPO from a backup, a Group Policy Administrator wizard walks you through the procedure.

The next step was to edit an offline version of the default domain Group Policy. Editing the "live" version of a GPO can be risky because any changes you make can be immediately seen by the objects (i.e., User, Computer) that are affected by that Group Policy. To protect the production AD, you shouldn't directly edit GPOs from within the NetIQ tool. Instead, edit them from within the GP Repository. The repository is empty by default. When you create a new GPO in Group Policy Administrator, it will originate in the repository and then be imported into the production AD. You must import existing GPOs (those you created before you installed Group Policy Administrator) into the repository if you want to edit them.

Once a GPO has been copied to the repository, you can check it out of the repository, edit it, then check it back in to the repository (multiple GPOs have to be mass imported via a script that Group Policy Administrator provides). I like the fact that Group Policy Administrator prompts the administrator to enter a comment when checking GPOs in and out of the repository. This kind of feature can be extremely valuable whenever a change management process is audited. After you edit a GPO from within the repository, you can run a report that compares the GPO in the repository to the one currently online in AD. Another useful report differentiates the two GPOs, pointing you to exactly where the differences are. Although the comparison report and the differential report sound as if they give the same information, they do not. The Group Policy Comparison report compares all the settings in the repository GPO to the online GPO's settings. The Differential report shows only the settings that differ between the two GPOs. These are power-

SUMMARY

NetIQ Group Policy Administrator 5.0

PROS: Lets you edit GPOs from within the tool; nice check-in/check-out feature

CONS: Must have Microsoft SQL Server 2000 or better (vendor-recommended MSDE isn't sufficient); must use a script to import multiple GPOs from AD into the GP Repository

RATING: ◆◆◆◆◇

PRICE: $900 for 100-user Active User License pack

RECOMMENDATION: An effective choice if you need an application that has a structured check-in and check-out procedure

CONTACT: NetIQ • www.netiq.com • 888-323-6768

Your potential. Our passion.®

Microsoft®

defeating witches. easy.

1. Boil, bubble, toil, and trouble.
Witches are big with brews. Why not make one of your own to use against them? Sure, eye of newt is tough to find at the local market, but it's probably available online.

2. Melt the Witch.
You've seen the film so you know the big ending. A bucket of water, poured directly Witchward, causes her to steam, melt, and dissolve into a puddle on the floor. Lure her to the watercooler and you're done.

3. Fight magic with magic.
With a wand of your own—say a pointer—you can create some magic of your own. Before you know it, you'll be turning Witches into toads.

4. Insult the Witch.
Witches, despite their warty exteriors, are quite sensitive. So asking "Hey, Witch—is that your nose or a green banana?" can be devastating.

5. Steal her broom.
Nearly every Witch has a magic broom, and if you can get it away from her she's basically grounded. And, with a little practice, you can cut your commute in half.

defeating worms. easier.

1. Implement Microsoft® Forefront.™
Forefront makes defending your systems easier. It's a simple-to-use, integrated family of client, server, and edge security products (such as ISA Server 2006) that helps you stay ahead of your security threats more easily than ever.

For case studies, free trials, demos, and all the latest moves, visit **easyeasier.com**

Microsoft®
Forefront™

ful reports that can help you identify problems immediately. The reports also help meet the next-to-last requirement in the change-management process I outlined earlier: verifying that the new GPO is in production.

The only feature Group Policy Administrator lacks is built-in audit functionality. The tool tracks the changes you make to the GPOs in the repository but doesn't track the GPOs that are in production. NetIQ has a product available for separate purchase called Group Policy Guardian that integrates with Group Policy Administrator and keeps track of production GPOs.

NetPro GPOADmin

NetPro's GPOADmin takes a different approach from the other two products in this review. Rather than creating a brand-new interface, GPOADmin extends GPMC. If you're already using GPMC, then you'll feel comfortable with GPOADmin, which Figure 2 shows. Like Group Policy Administrator, in order to use GPOADmin you must have SQL Server 2000 installed, and you'll also need the .NET Framework 2.0.

There are two setup applications on the GPOADmin CD-ROM: GPOADminExtensions.msi and GPOADminSetup.msi. GPOADminSetup.msi is the complete setup package to get your enterprise up and running. I chose to run it on my DC, but an enterprise would probably want to run it on a dedicated server in a production environment. Once GPOADmin is set up and running, you can use GPOADminExtensions.msi to extend the GPMC installations on your administration PCs.

Installing GPOADmin went smoothly and presented no problems. After the installation is complete, you are prompted to install a license file, which is a simple .txt file that you receive from NetPro. The import process for the license file took only a few seconds and went off without a hitch.

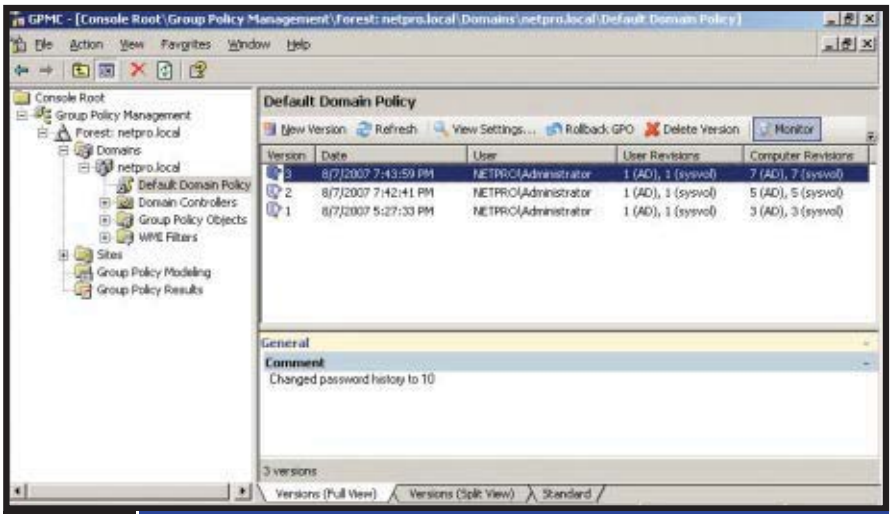


Figure 2: GPOADmin has the look and feel of GPMC

When you run GPOADmin the first time, you're prompted to install the following three components via a wizard: GPOADmin Database, GPOADmin Service, and the optional Monitoring Agent. I had no problems creating the database on SQL Server or creating the service that keeps track of the Group Policy activity. In the wizard, I chose to enable *Comments are required with GPO Version* because I wanted to see this functionality in action.

Testing GPOADmin

To begin my testing, I found the default domain policy and backed it up. The process in GPOADmin is nearly identical to Group Policy Administrator's process.

The next step presented my first problem: I couldn't find a way to edit the GPO offline. A quick review of the "Admin Guide" showed me what I was doing wrong: I was looking for a repository, or the word "offline" in the tool. But GPOADmin uses a "Lineage," which is a version history of each Group Policy. This way of rolling out new GPOs took a bit of getting used to because I didn't find it very intuitive.

The reporting in GPOADmin consists of numerous default reports that give such useful information as a listing of "Ineffective GPOs" (i.e., GPOs that aren't linked to an OU), Group Policy with "Cross-domain linked GPOs," and GPOs with duplicate links. You can also compare and contrast different GPOs to identify the differences between them. According to NetPro, GPOADmin "is the only solution with the ability to compare between two backups made with Microsoft GPMC so that organizations can leverage their investment with existing GPO backups." This is a useful feature for organizations that are already using GPMC.

One of the most intriguing features that I found while evaluating these products is GPOADmin's "GPO Cloaking." It allows you to stage new GPOs in production yet keep them hidden from administrators who don't have permission to see them. This feature prevents junior administrators from linking to and using a new GPO before it has been approved.

Extending GPMC is a slick idea and one that has paid off for NetPro. The only feature that I found to be frustrating was the implementation of Lineages. Given a choice, I would much prefer to have a separate repository to work from. Repositories give you a clear understanding of which GPOs are in production and which are not. Other than that, GPOADmin is a solid, clean product.

ScriptLogic Active Administrator

ScriptLogic's Active Administrator is the most expensive solution I evaluated, but it's also the most robust. It has most of the features the other products have, plus some additional ones. This product's tabbed interface was my favorite to work with.

Product setup, including standard installation questions, went off without a hitch. Active

SUMMARY

NetPro GPOADmin 1.5

PROS: Users of Microsoft GPMC will find this product immediately familiar.

CONS: Lacks a repository

RATING: ◆◆◆◆◇

PRICE: $6.00 plus $1.20 annual support and maintenance per user object

RECOMMENDATION: A strong choice for GPMC power users

CONTACT: NetPro Computing • www.netpro.com • 800-998-5090

netiq
An Attachmate® Business

Reduce the Headaches of Managing AD and Exchange

Migrate. Monitor. Manage.

Learn how to

Migrate, Monitor and Manage Exchange 2007

by downloading our new white paper:

www.netiq.com/go/exchange2007

Visit us at Windows Connections in Booth # 119.

SUMMARY

ScriptLogic Active Administrator 4.1

PROS: Can use MSDE 2000 or SQL Server in production; client-side troubleshooting; built-in auditing of Group Policy changes; simple folder structure for key components

CONS: Higher price than competitors

RATING: ◆◆◆◆◆

PRICE: Active Administrator 4.1 user license for minimum 50 users; $12.36 per user for one year of standard support

RECOMMENDATION: Its strong feature set, ease of use, and capabilities beyond GPO management make Active Administrator the tool of choice for companies that can handle its higher price.

CONTACT: ScriptLogic Corporation • www.scriptlogic.com • 800-813-6415

Administrator can use an MSDE back end to store its Security Event Database. However, MSDE has a maximum limit of five simultaneous connections. ScriptLogic recommends that you use SQL Server if "the combination of domain controllers and the number of users accessing the information will be greater than five." So, if you had two DCs and only three administrators *simultaneously* accessing data via Active Administrator, the MSDE database would work just fine.

Active Administrator stores non-security–related Group Policy data in an easily accessible folder structure. You are prompted to create this structure during the setup routine. I chose to install it on the root of the C drive: C:\aadata. This folder is automatically shared as ActiveAdministrator with a security setting of EVERYONE - FULL CONTROL. ScriptLogic recommends that you "modify the permissions of the share to only allow access by the service accounts used by the Active Administrator services, and by the users who will run the Active Administrator console." Doing so protects the data in these folders from being accessed by unauthorized users. I recommend that you create a security group called Role Active Administrators and assign this group Modify permission on the ActiveAdministrator folder. (To learn more about how to use role-based security, see "Let's Get Organized: File Server Basics," May 2007, InstantDoc ID 95354.) Don't forget to double-check your corporate backup settings to ensure that these folders are backed up regularly.

The folder structure of the ActiveAdministrator share looks like the following:

C:\aadata
- ActiveTemplates
- ADBackups
- GPOHistory
- GPORespository

The first subfolder stores Active Templates, which are similar to the Delegation Wizard that first debuted in Windows 2000. The ADBackups folder stores exactly what it describes: AD backups. GPO History is a feature that displays the names of everyone who changed a Group Policy and the date the changes were made. Both Group Policy Administrator and GPOADmin have a similar structure, but I liked how Active Administrator made the information easy to find.

Like Group Policy Administrator, Active Administrator has a GPO repository, which Figure 3 shows. But the Active Administrator Group Policy Offline Repository is stored in a folder structure, rather than on a database. This is the KISS (Keep It Simple Stupid) principle at its best—no database requirement or additional administrative overhead.

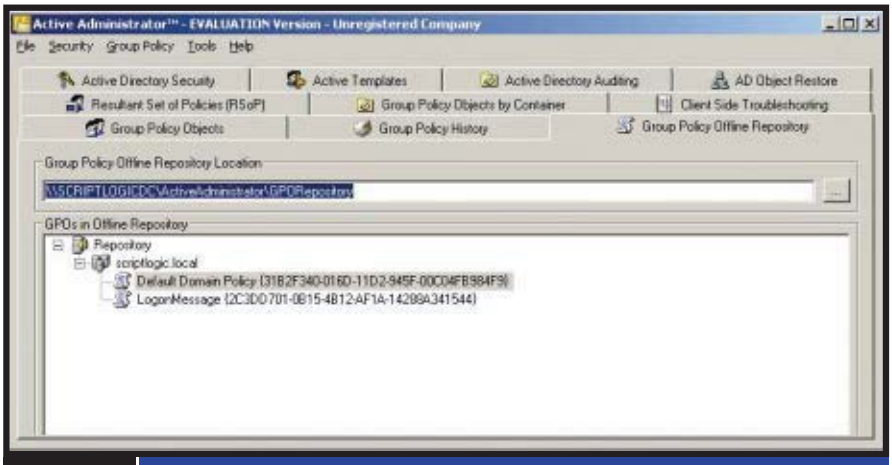


Figure 3: Active Administrator's Group Policy Offline Repository

Testing Active Administrator

I read the "Administrators Guide," familiarized myself with the product, and then ran through the mock change-management process. When I took a backup of the default domain policy, I immediately noticed a difference with this tool: When you right-click the policy name in the GUI and choose Backup, you have a number of choices:

1. Backup Security Group Filters
2. Backup Group Policy Links
3. Save a GPO Report
4. Generate Log File
5. Add additional Group Policies to backup
6. Schedule the backup

A simple backup and restore mechanism is a necessity for products of this type, but these advanced features set Active Administrator apart from the others.

I then copied the GPO to an offline area by using the Add to Offline Repository menu item. Once the GPO is in the repository it can be checked out, edited, and checked back in. The process is almost identical to Group Policy Administrator except that Active Administrator doesn't prompt you to add notes.

When it comes to auditing what has happened with Group Policy, Active Administrator has a clear lead on the competition. By using an Active Administrator agent on each DC, you can keep a close eye on who's doing what with Group Policy. In addition to Group Policy changes, Active Administrator will let you know who has reset a password, deleted a user, and performed other administrative actions. You can capture, track, and report on more than 80 security events. If your company requires you to audit whether Group Policy follows your change-control process, then Active Administrator is the clear choice for your environment.

Active Administrator's tabbed interface is extremely easy to master. Each area is clearly labeled, and I found Active Administrator the easiest tool to hit the ground running with.

However, added features that are outside the scope of Group Policy management make Active Administrator an expensive option.

Reviewing the Pros and Cons

All three products do a good job of improving the Group Policy management process, but each does so in a different way. Group Policy Administrator and Active Administrator both use an offline repository to let you work on GPOs in an offline environment. Group Policy Administrator stores its repository in a SQL Server database. Active Administrator uses a file system as an offline repository. GPOADmin, in contrast, is an extension of GPMC and doesn't use a repository at all. Instead, GPOADmin backs up a GPO automatically before you start editing and after you finish editing. This tool is geared toward customers who don't want to modify existing GPOs by following the model that says you replicate an existing GPO, make changes to it, and when you're ready to deploy it, link it where the existing GPO is and then remove the links to the old GPO. GPOADmin's approach is different because the product satisfies a different set of customer requirements.

All three products require a back-end database. Group Policy Administrator's repository is in SQL Server. GPOADmin's database stores backups and old versions of live, production GPOs in its database. Active Administrator's database stores security events such as editing, adding, or deleting GPOs, as well as other security-related events.

The look and feel of each product is unique. Group Policy Administrator looks like an extension of GPMC, whereas GPOADmin really is an extension of this Microsoft tool. Active Administrator doesn't look like either Group Policy Administrator or GPOADmin but resembles the properties of a User object in AD with its tabbed layout.

The reporting capabilities of each product were similar. All three of these tools will help you find the similarities and differences between GPOs.

My Bottom Line

If you administer Group Policy in a medium to large company, then you're probably familiar with the frustration of not having the tools you need to manage Group Policy in a change-control environment. All three of these products can help you get your GPOs organized in a structure that you can easily manage. NetIQ's Group Policy Administrator and NetPro's GPOADmin are both strong products. But because ScriptLogic's Active Administrator had the best look and feel, was the most intuitive, and includes extra features to help manage Group Policy, I designate it my Editor's Choice.

InstantDoc ID 97228

Eric B. Rux

(ebrux@WHSHelp.com) is cofounder of WHSHelp.com. His monthly column "Coming Home: Thoughts on Windows Home Server" can be read at www.connectedhomemag.com. Eric is a senior Windows Administrator and teaches the Microsoft Certified Systems Administrator (MCSA) program at a tech college.

HIT MALWARE. HARD.

NEW V3! With 'Malware Command Center'

Windows IT Pro READERS CHOICE 2006 Winner

Network Computing 2006 WELL-CONNECTED AWARDS WINNER

Product Excellence Awards 2007 Info Security Products Guide CUSTOMER TRUST

Is your network protected against blended malware threats? Cyber criminals are using combinations of spambots, worms, trojans, rootkits and social engineering to infect your users' machines. Spyware has morphed into malware. You need protection against these new security threats.

Surveys show one of the biggest security issues admins see this year is blended malware. Protecting your network from the loss of confidential data, employee productivity, and network bandwidth is a major issue.

CounterSpy Enterprise: The most powerful antimalware available: Company-wide malware protection requires a real, centralized enterprise product. CounterSpy Enterprise is just that: a scalable, policy-based tool that delivers a new, revolutionary hybrid antimalware technology that provides robust protection against blended threats.

Hybrid antimalware engine with VIPRE technology: CounterSpy Enterprise is powered by a hybrid engine that merges classic spyware detection and remediation with Sunbelt's new Virus Intrusion Protection Remediation Engine. VIPRE has traditional antivirus and cutting-edge antimalware techniques. The upshot? Faster scanning and dramatically less system resources.

Customized 'Malware Command Center': With CounterSpy Enterprise's new configurable management dashboards, you can easily create a customized 'malware command center' that gives instant access to your most used reports and policy controls. Four customizable dashboards provide at-a-glance views of scanning and remediation activities that show the overall health and performance of your network.

Kernel-level Active Protection: CounterSpy Enterprise's Active Protection™ offers signature, behavioral and heuristic-based real-time blocking of threats. It works seamlessly with existing desktop antivirus solutions. And it has the best threat database in the industry. Period.

Download your evaluation copy at:
www.sunbeltsoftware.com/csewin

Sunbelt Software

COUNTER SPY ENTERPRISE

Find out how many machines in your organization are infected NOW!

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbeltsoftware.com sales@sunbeltsoftware.com

Exchange Server Monitoring Tools

Track system health and performance to save time

As an Exchange Server administrator, you need to keep your organization running at peak performance, and you probably don't have the necessary staff or budget. You certainly don't have time for email failure or downtime. Using a software solution can help you monitor your Exchange environment. Many products exist to fill this role, and they come with a variety of capabilities.

What Do You Expect It to Do?

You might start your search for a monitoring solution by asking yourself what you really need it to do. At the most basic level, you need a tool that tracks the health and performance of your system. If something is causing a traffic bottleneck for messages traversing your network, you'll want to know where it is and what's causing it. Many products can probe the system and report email transit times, but that doesn't mean they can actually pinpoint a problem. Some products, such as Permessa's **Email CONTROL! for Exchange (ECX)**, can analyze message routing within the environment to ensure efficiency.

Another important consideration is whether the management software operates proactively or reactively. Ideally, you probably want to find a solution that will identify developing situations and send you an alert before the problem can affect your network, giving you the chance to take preventive action. However, in some environments, it might be enough that you can manually pull a report to show the system status. The goal, of course, is to avoid network downtime and thereby enable optimum user productivity. In fact, some Exchange management software products include the ability to take corrective action. For example, **Argent Exchange Monitor** can restart services for you and even reboot failed servers, all based on criteria you set up.

How Easy Is It to Use?

Your Exchange monitoring solution is intended to save you time and effort, so be sure to select software that is itself easy to manage. The big question is whether the product requires an agent to be installed. In some organizations, installing an agent might not be an option because of security or bandwidth concerns. Plenty of agentless or agent-optional products are available, so you should be able to find something that meets your needs. Some products, such as **Heroix Longitude**, can auto-discover your system's elements on installation, making configuration easier.

Certain Exchange monitoring solutions are provided as modules of larger system management products. For example, **NimBUS** works only with the separate NimBUS service level management application. If you're already using the overarching product, then choosing the module for Exchange management might be an easy decision, letting you combine management functions into a single interface.

The solution you choose should be customizable to meet your needs. You might want to schedule data collection from the Exchange network for nonpeak hours, for instance. Do you have a choice of alerting options that makes sense for your operations? Does the solution provide the reports you need, or does it feature a custom reporting tool that will let you create them? These could be the critical considerations for your environment.

Will It Continue to Meet Your Goals?

When you choose a management solution, you want to be sure it's right not only for today but also as your organization grows and changes. Choose a product that's scalable to your needs: If you plan on your organization doubling in size over the next three years, you'll need to be sure your management solution is ready for that challenge.

Something that a lot of organizations are contemplating—if they're not already committed to it—is the upgrade to Exchange Server 2007. This might be something you'll need to keep in the forefront of your mind as you investigate management solutions. You don't want to install software that works only with Exchange Server 2003 if you think you'll be migrating in the foreseeable future. Many companies have added support for Exchange 2007 to their management products over the past year, and others have it in the works. Keep in mind that Exchange 2007 has a new role-based architecture and new management based on Windows PowerShell. "Support" for Exchange 2007 doesn't necessarily mean a product will help you with new challenges arising from these changes.

The Bottom Line

Every organization is different, and every administrator has different needs—and budgets. The tool that's right for you and your business is a choice you have to make according to your preferences and the demands your organization places on you. Choosing an Exchange monitoring solution shouldn't add stress to your busy day. Use these guidelines and the product table on pages 32-33 to get your search started in a positive direction.

InstantDoc ID 97151

B. K. Winstead (bwinstead@windowsitpro.com) is an assistant editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in messaging and unified communications.

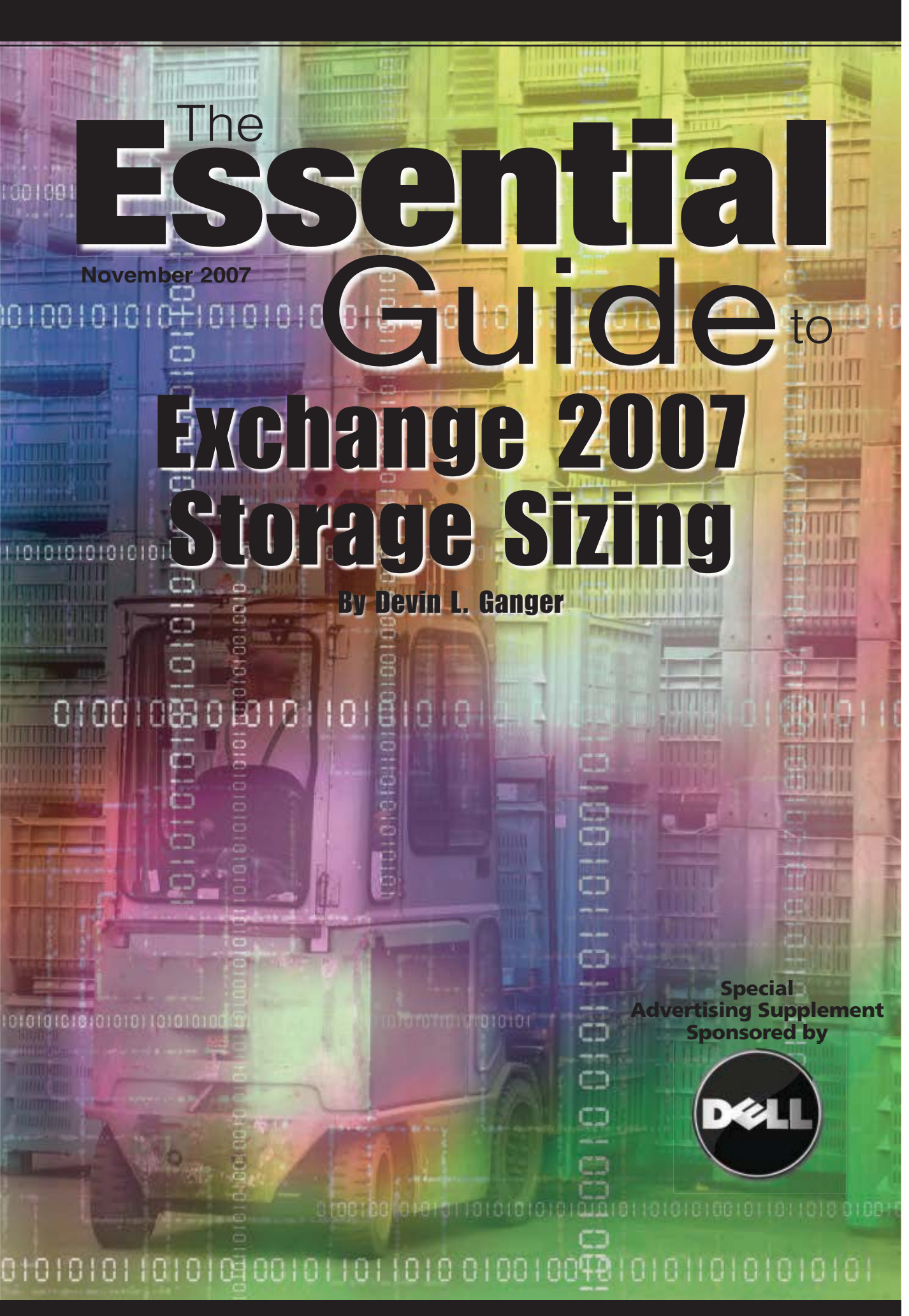
EDITOR'S NOTE

The Buyer's Guide presents vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to www.windowsitpro.com/buyersguide.

Company	Product	Price	Exchange Versions Supported	Agent Required?	Module or Standalone Product?	Items Monitored	
						Send failures	Send/receive timeouts
Argent Software 860-674-1700 www.argent.com	Argent Exchange Monitor	$3,000 per server	All	No	Standalone	Yes	Yes
CA 800-225-5224 www.ca.com	CA Unicenter Management for Microsoft Exchange	$2,120 + cost per mailbox	Exchange 2003/2000	Agent and agentless options	Module and standalone	Yes	Yes
Ensim 877-MY-ENSIM 408-496-3700 www.ensim.com	Ensim Unify Enterprise Edition	$20 per user per year	Exchange 2007/2003	No	Standalone	No	No
Heroix 800-229-6500 617-527-1550 www.heroix.com	Longitude	Starts at $299	Exchange 2003/2000	No	Standalone	No	No
HP 800-888-9909 www.hp.com	HP OpenView Smart Plug-in for Microsoft Exchange Server (Exchange SPI)	Starts at $800 per managed system; starts at $15,000 including HP Operations Manager	Exchange 2007/2003/2000	Yes	Module	No	No
Microsoft 800-MICROSOFT (642-7676) www.microsoft.com	Microsoft System Center Operations Manager 2007	Contact vendor	Exchange 2007/2003	Yes	Standalone	Yes	Yes
Nimsoft 877-752-6468 650-570-5401 www.nimsoft.com	NimBUS	Starts at $750	Exchange 2003	Yes	Module; works with NimBUS service level management application	Yes	Yes
Permessa (formerly DSY Analytics) 781-694-2200 www.permessa.com	Email CONTROL! for Exchange (ECX)	$1,995 for up to 1,000 users; $2,625 for up to 2,500 users; $3,275 for up to 5,000 users; $6,400 for up to 10,000 users	Exchange 2003/2000/5.5	No	Standalone	Yes	Yes
PROMODAG 888-696-5404 33-1-53-27-66-60 www.promodag.com	PROMODAG Reports	Starts at $755	Exchange 2007/2003/2000/5.x/4.0	No	Standalone	Yes	Yes
Quest Software 800-263-0036 614-336-9223 ext. 1 www.quest.com	MessageStats	$12 per mailbox	Exchange 2007/2003/2000/5.5	No	Standalone	Yes	Yes
	Spotlight on Exchange	$5 per mailbox	Exchange 2007/2003/2000/5.5	No	Standalone	Yes	Yes
Zenprise 888-936-7747 www.zenprise.com	Zenprise for Exchange	$35 per user for 1,000 users	Exchange 2007/2003/2000	No	Standalone (integrates with Microsoft Operations Manager)	Yes	Yes

*See product documentation.

EDITOR'S NOTE: Some vendors that you might expect to see in this Buyer's Guide said they didn't have a product that exactly matched the criteria or didn't



The Essential Guide to Exchange 2007 Storage Sizing

November 2007

By Devin L. Ganger

Special Advertising Supplement Sponsored by

DELL

If you have experience with previous versions of Exchange Server, you may find that deploying Exchange 2007 is an interesting exercise in combining the familiar and the new. On the one hand, there are many aspects of the planning and deployment process that feel similar to Exchange 2000 and 2003; on the other hand, there are whole new concepts to master and major changes to learn. The move to a 64-bit architecture in Exchange 2007 has ushered in some amazing improvements in the scalability and performance of Exchange 2007 storage designs.

Whether you're familiar with Exchange storage sizing already or coming to it fresh, proper storage sizing continues to be critical to the success and long-term health of your Exchange 2007 deployment. Mistakes in storage sizing can be difficult and costly to fix, and there's a lot of confusion and myths floating around. In this guide, I'll explain the fundamental concepts underlying Exchange storage sizing, explore the relationship between storage performance and capacity, and show you which factors you need to consider as you're planning your Exchange 2007 storage deployment.

Mailbox Performance

Contrary to popular belief, once you get beyond 50-100 mailboxes, your storage system performance can become far more important to your Exchange deployment – and the experience your users have – than its total disk capacity. Don't get me wrong; capacity is important and I'll talk about it later, but I want to emphasize that you can't accurately calculate your storage needs if you don't understand how Exchange uses its storage and where the potential performance bottlenecks come from.

There's a common school of thought that buys the largest hard drives available, deploys them in the most space-efficient RAID configuration possible, and calls it good enough. People who follow this line of thinking usually either end up troubleshooting a slow, unusable system or spending too much money (or both), all because they don't understand the principles of Exchange performance.

Mailbox Databases and Storage Groups

The heart of understanding Exchange performance and sizing lies in understanding the separation between mailbox databases and storage groups.

- Mailbox databases are ESE database files that hold the actual mailbox data for one or more mailboxes. These databases are specifically designed to hold mailbox data in pages, blocks of memory 8KB in size (doubled from Exchange 2003's page size of 4KB). While mailbox databases are designed to support random read and write operations as users retrieve items, make changes, and receive new messages, this page size allows disk access to be more efficient by reducing the amount of seeking the drive head must perform between operations. The page size dictates the smallest amount of data that is read or written in any I/O operation. It's more efficient to read and write larger blocks of data if the page size smaller than the average total request. E-mail messages are now most often larger than 4KB. These messages can be stored in Exchange 2007 using half as many pages (and thus half as many I/O operations) as in Exchange 2003.
- Storage groups are containers that hold one or more mailbox databases. However, they also fulfill another important function: they hold the transaction log files for all databases in the storage group. When a write must be performed to a mailbox database, Exchange doesn't just directly make the write; it instead writes the transaction to the relevant transaction log file. In previous versions of Exchange, these files were exactly 5MB in size; in Exchange 2007, they have been reduced to 1MB. The use of transaction logs increases performance by using sequential write operations to complete the transaction while wasting minimal time on disk seek operations. Exchange 2007 lowers the transaction log size to provide better efficiency, and more granularity, for its built-in continuous replication features.

One of the big changes in Exchange 2007 is that now you can create a separate storage group for each database, up to the maximum number of databases you can create with your version of Exchange; with Exchange 2003 you were limited to a maximum of four storage groups, each of which could hold up to five databases. In Exchange 2007 Standard Edition, this means you can create up to 5 databases and storage groups; in Enterprise Edition, this increases to 50 databases and storage groups. Note that these numbers are totals (e.g. you can have 2 storage groups with 25 databases, 5 storage groups with 10 databases, or 50 storage groups with 1 database each).

There are many implications to creating a separate storage group for each mailbox database:

- One of the biggest is the ability to backup and restore your mailbox data. When each mailbox database has its own set of transaction logs, your backup and restore operations have a huge advantage; you can perform full backups at the database level and remove unneeded transaction log files. Without this full backup, your log files will not be deleted and you'll eventually run out of drive space.
- With a single database's transaction logs to worry about, Exchange has to apply changes to the database less frequently, resulting in even more better performance.
- One of the long-standing Exchange storage best practices is to place mailbox databases and transaction logs on separate arrays or LUNs. Because they have completely different I/O patterns, separating them allows each related set of drives to perform the type of I/O it's best configured for.
- If you have a large number of databases and follow

the advice to place each database and storage group on its own volume or LUN, you will quickly have a large number of disk volumes to manage. You should use NTFS volume mount points to allow these volumes to be mounted as folders, rather than using (and running out of) the limited number of drive letters you have available.
- If you're using SAN-based storage, you need to be careful about how you create the LUNs for Exchange; Exchange LUNs should never share the same physical disks with other applications.

Calculating Performance

The unit we measure Exchange performance with is I/O operations per second, or IOPS. This is, quite simply, a measure of how many read and write operations a storage system can perform in a second. There are many factors you must consider when calculating the total IOPS load your Exchange storage system must support and design your storage system appropriately:

- Number of mailboxes. This one is pretty obvious; the more mailboxes you have in the same mailbox databases, the more IOPS it will take to meet the load on that database. Mailbox size, on the other hand, doesn't affect IOPS load (but it does affect the database size).
- User behavior. There are actually two factors here: how heavily do your users hit their mailboxes, and how many of them do you expect to be connected to Exchange at one time on average? Microsoft has a list of mailbox use profiles and IOPS baselines at: http://technet.microsoft.com/en-us/library/bb738147.aspx. The mode with which users connect to their mailboxes can also be a factor; Outlook's cached Exchange mode tends to spread out the IOPS load more than online mode does.
- Type of disks. Each disk has a maximum IOPS it can support. SCSI, FC, and SAS drives usually support more IOPS than comparable IDE and SATA drives because they are optimized for server-grade workloads; faster drives (15KRPM) support more IOPS than slower drives (10KRPM and 7200RPM) because they reduce the seek time between concurrent operations.
- RAID configuration. It seems that every Exchange expert has their own advice about which RAID configuration to use for which volume and what it all boils down to is this: does your configuration provide a good match to the IOPS levels and I/O characteristics of your volumes? Each RAID configuration has its own pros, cons, and implications for IOPS.

Here's the basic rule of thumb for mailbox database IOPS: (# of mailboxes) x (Mailbox profile baseline IOPS) x (Concurrency %) = (Total IOPS)

That's just the IOPS for the database; this capacity then should be split into read IOPS and write IOPS. If you follow Microsoft's memory sizing recommendations, you can assume this ratio is 1:1 reads to writes; otherwise, use a factor of 2:1 when doing your initial planning. The Exchange documentation gives a far more detailed method if you need greater precision.

Once you have the write IOPS for the database, you can calculate your log IOPS: (DB Write IOPS) x (3:4 log to DB write ratio) x (20% burst overhead) = Log IOPS

Here's an example: your mailbox database has 1,500 mailboxes, all at the Heavy usage profile with an IOPS per user of .32, and 75% concurrency. Your storage design for this database must provide a total capacity of 360 IOPS for the database (1,500 x .32 x .75 = 360). Assuming the 1:1 ratio, this gives us 162 IOPS for the log (180 x .75 x 1.2 = 162). You might be able to satisfy this with a single drive; more likely, you'd need multiple spindles to provide the necessary performance.

The Effect of Memory

The switch to 64-bit support shows its greatest effect in how Exchange 2007 makes use of physical memory. Exchange aggressively loads database pages into cache and keeps a map of updated blocks in memory. As changes are applied and written to the transaction logs, Exchange will wait for opportune moments to write the changes back to the mailbox database. By using a combined transaction log/cache strategy, Exchange consolidates these write operations to minimize wasted I/O. Exchange 2007 is no longer bound by a hard 4GB limit and can cache far more data than previous versions, further reducing the I/O demands.

However, there are a combination of factors that produce a new "sweet spot" for Exchange memory usage. The first is cost; at current memory prices, it quickly becomes cheaper to add more disks rather than move beyond 32GB in many server configurations. The second is the impact of non-transactional operations such as online maintenance, backup operations, and mailbox management; caching has little effect on reducing the I/O demands of these operations. (However, most of these operations should be scheduled to take place during non-peak times, so their impact on ordinary operations may be negligible.) The third is the fact that Exchange 2007's caching works best after the server has been operational for long enough to populate its cache; beyond 32GB, it may take too long to cache enough data to provide significant results.

The Exchange 2007 documentation gives a series of recommendations for memory sizing. If you don't follow these recommendations, your Exchange server will not be able to adequately reduce its IOPS requirements and will consequently demand more performance from your storage system. Following Microsoft's memory guidelines can dramatically change the I/O performance of the system; if you give it enough memory for caching, your read/write

ratio will be close to 1:1 (50% reads); if the server doesn't have enough memory, the read/write ratio trends closer to 2:1 (66% reads).

Continuing our previous example, our 1,500 Heavy users each require an average of 5MB of cache RAM – an approximate total of 7.3GB on top of the 2GB baseline requirement for the Mailbox role – a total of at least 9.3GB of RAM if we want to get the best effect from caching. Looks like this server is a 10GB server!

High Availability Considerations

When you're using the high availability configurations such as LCR, CCR, and SCR that make use of log replication, there are a couple of extra considerations:

- The 1:1 ratio of databases to storage groups is usually a requirement for these configurations, not merely a good idea.
- You should add an additional 10% IOPS overhead to the corresponding log volume to account for the log file reads the replication process requires. In addition to our 162 IOPS for log writes, we need to plan for 16.2 IOPS for log reads when using LCR, CCR, or SCR.
- Don't forget to evaluate the IOPS capability of the passive node of a CCR cluster, or on the target of your SCR replication setup.

Mailbox Capacity

Now that you know your performance targets, you have an idea how many disks you need to have in your storage system to meet the I/O requirements. The next step is to figure out the total disk capacity you need, thus telling you what size of disks you need to buy. This process is quite a bit more straightforward than performance sizing. For Exchange 2003, it was not uncommon to see storage configurations that had an excess of disk capacity in order to meet the performance requirements. With Exchange 2007's better caching, this disparity should be smaller (or, ideally, non-existent).

Sizing mailbox database volumes

As with capacity, there are many factors to take into account when you're looking at the total disk capacity your Exchange database volumes will require:

- **Number of mailboxes.** This one is pretty obvious; the more mailboxes you have in the same mailbox database, the more disk space you'll need on the database volume in order to store them all.
- **Mailbox quota.** Mailbox size plays a key role in capacity sizing. You want to set some limits so you can manage capacity effectively, but don't be so stingy that your users don't have enough room. It's a good idea to apply quotas, even if they're very large, to help make space use more predictable. For example, a 2GB quota probably won't inconvenience your users (unless they already have huge mailboxes), but it will help you plan an upper limit for your storage needs on your servers.
- **Database white space.** The Exchange database reclaims pages that have been freed up and marks them as available, but it doesn't physically shrink the size of the database file. You can estimate the whitespace by the total amount of mail sent and received in one day by the mailboxes in the database, or you can check the system event log for event ID 1221 to see how much white space is left after online defragmentation finishes.
- **Deleted item retention.** The dumpster is a feature of the database that allows users to recover items they've really, truly deleted for up to a set number of days. This is a configurable value with a value of 14 days; the longer you set it, the more space it requires, approximately equal to the number of days multiplied by the message delivery rate.
- **Content indexing.** Content indexing uses approximately 5% of the database size to maintain the index files.
- **Maintenance.** Offline maintenance and database recovery can both require extra room. You should allocate at least 110% of the space of the largest database on the volume to provide enough space for these activities.
- **Growth.** It's generally wise to leave some wiggle room to allow future growth of your databases—usually around 20%.

The rule for planning the average mailbox size is:
(mailbox quota) + (dumpster size) + (2 weeks of incoming mail) = mailbox size

Once you know the average mailbox size, you can determine your mailbox database volume size:
(# mailboxes) x (mailbox size)= baseline DB size
(baseline DB size + whitespace) x (+5%) x (+110%) x (+20%) = total DB volume size

Let's continue the example. We have 1,500 Heavy mailboxes; we'll say we have a 1GB quota and that each user sends and receives 100 50KB messages per day.

That puts our average mailbox dumpster at 54.7MB (14 x 80 x 50KB = 56,000KB) and our average mailbox size at 1.1GB (1024MB + 68.4MB + 54.7MB = 1147.1MB). That makes the baseline database size is 1.6TB (1,500 x 1.1GB = 1,650GB).

Our whitespace equals 7.2GB (1,500 mailboxes x 100 x 50KB = 7,500,000KB). Adding it all together, we get 4.2 TB (1,650GB + 7.2GB) x 1.05 x 2.1 x 1.2 = 4,385GB). You can probably get away with less space if you're willing to reduce the 110% free space requirement; in that case, you'd only need 2.09TB, but the reduced space might make repair operations more difficult.

Sizing mailbox log volumes

Once you know how large your mailbox database volume is, you next need to calculate how large your log volumes will need to be. The log volumes need to be large enough to store all of the transaction logs created

between backup intervals, or to facilitate mailbox move operations. One would think that log volume size could be simply calculated by taking the size of all of the e-mail messages sent and received during a day, then taking that number and multiplying it by the number of days of logs that you might need to store. This provides a simple first-cut estimate, but it won't be very precise. There are messages and objects that are stored in mailboxes that are not messages, and that might never be sent or be received. Examples include server-side rules, safe and blocked sender lists, OOF messages, and other hidden items. To properly account for unsent and unreceived messages, log volumes should be calculated based on the mailbox profiles in the database. See the following table to see the estimated number of log files generated per day per profile.

Mailbox Profile	Messages Sent and Received per Day	Logs Generated per Mailbox per Day
Light	5 sent/20 received	7
Average	10 sent/40 received	14
Heavy	20 sent/80 received	28
Very Heavy	30 sent/120 received	42

Number of transaction logs generated for each mailbox profile

Note: This table is based on an average message size of 50kb. As the average message size goes up, so too will the number of log files generated. At 100KB you need to multiply the logs generated by 1.;, at 200KB you need to multiply by 2.8 (double the multiplier); at 300KB you need to multiply by 4.6, and so on.

To calculate the log volume size based on the Microsoft recommended method you take the number of log files generated per user per mailbox profile, and multiply that by the number of users in the database, then multiply that by the number of days between backups. It's a good idea to add in a 20% buffer just in case there is extra volume generated during the day above your averages. The formula looks like this:
(Message Profile Logs Generated x Number of Users) x (Days Between Backups) x (+20%) = total Log volume size in MB

Back to our example of 1,500 heavy users; we will assume a 50KB average message size for all of the users, giving us a logs generated number of 42 per day per user. 42 x 1,500 = 63,000 x 1.2 = 75,600 log files per day. We'll be running backups once a day so 75,600 is the number of log files that we need to scale our disks to hold. Log files are 1MB each, that makes simple math and means that we need 75.6GB of space for our log volume.

Other roles

The Mailbox role isn't the only role you need to worry about in an Exchange 2007 organization. You also need to ensure that the other four roles also have adequate disk sizing to perform their functions.

Transport roles

The obvious roles you first want to look at are the Hub Transport and Edge Transport roles. In Exchange 2003, bridgehead queues used a simple folder on an NTFS partition to store messages in transit. In Exchange 2007, the queues are now also an ESE database and transaction log, again to increase performance.

Exchange 2007 introduces the concept of backpressure; if Exchange detects that the server is running low of crucial resources such as free disk space or memory, it will start to temporarily reject messages and give itself a chance to work through the backlog of messages. One of the easiest ways to trigger backpressure is to not have enough disk space on the transport server; the Exchange Transport process wants to have at least 4GB of free space at all times on the drive that hosts the queue database in order to ensure adequate room to store incoming messages and hold them for a period of time.

Additionally, the queue database includes a transport dumpster. Messages that have been received and forwarded on aren't immediately deleted; they are placed in the transport dumpster. These messages can then be retrieved in the event that a CCR-enabled mailbox cluster has to perform a failover and needs the last few minutes of delivered messages to be resent.

On busy transport servers, you may want to move the queue database, queue log files, and message tracking logs to separate disk volumes. The Microsoft Exchange 2007 documentation includes sizing guidelines to assist you in determining how large these volumes should be.

Client Access Server role

The Client Access Server role doesn't use much disk space for anything except the HTTP access logs. For performance and better retention, you may wish to move these logs to a separate disk volume.

Conclusion

Properly sizing Exchange is a complicated process; to do it well, you need to have some good usage numbers for your user population and the willingness to take some time instead of just buying the largest RAID arrays your budget will allow. It's worth doing it correctly, though; the little bit of extra time you take up front will save you a lot of time down the road trying to compensate for an inadequate design.

Devin Ganger is a messaging architect for 3sharp, an Exchange MVP, and co-author of *The Exchange Server Cookbook* (O'Reilly and Associates).

STOP PAYING FOR TOOLS YOU DON'T NEED

ONLY DELL OFFERS A MODULAR APPROACH TO UNIFIED COMMUNICATIONS

Using Unified Communications is a smart move. Buying more components than you need isn't. Only Dell offers an "à la carte" approach so you can add powerful messaging features as you need them. So get started with Unified Communications today—your way.

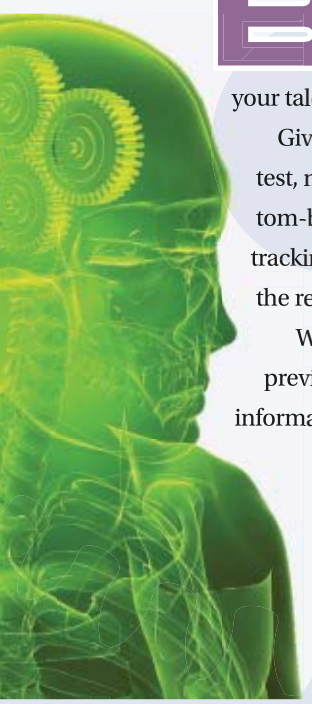
SIMPLIFY COMMUNICATION AT DELL.COM/Unified

	Mailbox/ folder size	Disk capacity	Disk utilization	Mailbox limits	Protocols Monitored	Reporting	Problem-Escalation Features?	Alerts						New Features (past 12 months)
								Email	Pager	SNMP	SMTP	SMS	Other	
	Yes	Yes	Yes	Yes	SMTP, MIME, POP, IMAP	Email traffic analysis, performance trends, service level agreement (SLA)	Yes	Yes	Yes	Yes	No	Yes	Yes*	Exchange 2007 support; BlackBerry server ruleset; new alerts
	Yes	Yes	Yes	Yes	IP, SMTP, MAPI	Email traffic analysis, performance trends	Yes	Yes	Yes	Yes	Yes	No	No	Discovery subsystem; Web-based UI; silent install
	Yes	Yes	Yes	Yes	POP, IMAP4, SMTP, MAPI, HTTP	Usage and capacity utilization, audit	Yes	Yes	No	No	No	Yes	No	New product
	Yes	Yes	Yes	Yes	SMTP, DHCP, and monitor availability of port	Email traffic analysis, performance trends, SLA	Yes	Yes	Yes (via email or third party)	Yes	No	No	No	Annotated SLAs and reports; topology-based network representation; auto-discovery and other scalability enhancements; VMware monitoring and other expanded coverage
	Yes	Yes	Yes	Yes	IMAP4, POP3, SMTP, DAV, NNTP	Email traffic analysis, performance trends, SLA	No	No	No	No	No	No	Scripts, trouble ticket generation	Exchange 2007 support, including support for custom cmdlets and additional graphs and reports
	Yes	Yes	Yes	Yes	SNMP, Syslog, WS-Management	Email traffic analysis, performance trends, SLA	Yes	Yes	No	No	Yes	Yes	IM	New product
	Yes	Yes	Yes	Yes	SMTP, POP3, MAPI, IMAP, HTTP, NNTP, LDAP, DNS	Email traffic analysis, performance trends, SLA	Yes	Yes	Yes	Yes	No	Yes	Yes*	Support for Exchange clusters
	Yes	Yes	Yes	Yes	N/A	Email traffic analysis, performance trends, SLA	Yes	Yes	Yes	No	Yes	No	No	N/A
	Yes	Yes	Yes	Yes	OWA	Email traffic analysis, performance trends, SLA	No	Yes	No	No	No	No	No	Support for Exchange 2007, Windows Vista; exports to SharePoint; report for appointment search for a given date range
	Yes	Yes	Yes	Yes	N/A	Email traffic analysis, performance trends, SLA	No	No	No	No	No	No	No	Add-on report packs for reporting on other messaging components (Sendmail, Postfix, OWA, BlackBerry, archive)
	No	Yes	Yes	No	SMTP, RPC (MAPI), POP3/ IMAP4, MTA, HTTP (OWA)	Email traffic analysis, performance trends, SLA	Yes	Yes	Yes	No	No	No	No	Support for non-Exchange servers; enhanced diagnostic console
	No	Yes	Yes	Yes	SMTP, POP, IMAP, MAPI	Email traffic analysis, performance trends, SLA	Yes	Yes	Yes	Yes	No	No	Console	VIP dashboard to monitor critical users; end-to-end view of BlackBerry infrastructure problems; addition of problem signature files from the RIM knowledgebase and Zenprise experts; new reporting capabilities

respond to our requests for information about their products.

Windows IT Pro INNOVATO Share Their Successes

For the third year in a row, we recognize hard-working IT pros and their resourceful technical solutions by Anne Grubb and Jeff James



By definition, IT is a behind-the-scenes profession. Your non-IT coworkers take IT services and your skills for granted—unless, of course, email isn't working or the network dies, and then suddenly all eyes are on you. Although most IT folks didn't get into the career to become rock stars, at *Windows IT Pro*, we believe your talent for solving problems and understanding technology is worthy of recognition.

Giving IT professionals the appreciation they deserve is the main intent of the *Windows IT Pro* Innovators contest, now in its third year. Among this year's winning entries are an automated Web-site creation solution, a custom-built internal portal, two solutions that greatly simplified complex software upgrades, and two methods for tracking users' access to systems and applications. The common thread among this diverse group of solutions is the resourcefulness of the IT pros who created them, using their problem-solving skills and the tools at hand.

We hope this year's award winners will inspire you when you're dealing with your own IT challenges. As in previous years, we've published the winners' email addresses, so feel free to contact any of them if you want more information about their solutions.

GRAND PRIZE WINNERS

Creating Web Sites in a Snap

At most universities, staff, students, and teachers rely on the Web for disseminating college and course-related information. Instructors and professors publish class schedules, assignments, lecture notes, and students' grades on their Web pages. Staff maintain college and division sites with news and forms for current and potential students. With thousands of sites and hundreds of requests pouring in, keeping up with the demands was straining the University of Wyoming's small IT staff, as Systems Programmer Rowdy Downey explains. "We were getting 25 to 50 requests per week to manage sites for authors. We have thousands of professors, departments, colleges, units, classes, projects, and so on, all wanting to set up, delete, or manage configurations for their sites. Fulfilling these requests quickly became a massive drain on our time, so I decided to automate the site-creation process."

Rowdy launched the project by first investigating whether an existing product could do the job he required. "We wanted to create sites that were sandboxed, secure, manageable, and flexible," he says. "I couldn't find any [product] robust enough to meet our requirements." Rowdy believed he could build the solution himself, but before he could begin development, he spent a lot of time researching blogs and Microsoft and scripting sites to find the tools, scripts, and techniques he'd need.

Rowdy's solution consists of a combination of ASP and ASP.NET, plus several Microsoft utilities (adsutil.vbs, iisvdir.vbs, xcacls.vbs, owsrmadm.exe, rmtshare.exe, and sleep.exe), all tied together in a 2,388-line VBScript program. "Although this seemed like a relatively simple automation solution, it quickly proved to be quite involved," says Rowdy. "The solution needed to be able to create and configure groups, set permissions for sites and databases, set ODBC connections, set metabase configurations, create IIS sites, extend sites with Microsoft FrontPage extensions, create shares, and set share permissions."

The utility uses the university's Active Directory (AD) infrastructure and properties set on


RS

various universal groups to control authoring and browsing to specific sites. Rowdy developed secure Web interfaces through which faculty, staff, and students can submit requests to create, delete, and manage site properties. Scheduled jobs launch the utility to perform the actual work. The solution handles multiple site-configuration options, including basic sites, FrontPage-extended sites, multimedia streaming sites, calendar sites, development sites, data-access capabilities, site-browse restrictions, and forced Secure Sockets Layer options. This same utility has been ported to provide University of Wyoming students personal sites that they use for portfolios, class assignments, and graduate projects, all with the benefit of automated administration to minimize resource drain.

Hosting the numerous on-campus sites in a secure, sandboxed environment requires running hundreds of application pools concurrently in Microsoft Internet Information Services (IIS) 6.0. This approach has revealed certain architectural limitations of Windows. Rowdy says that moving to 64-bit hardware will ultimately alleviate these problems.

Rowdy
DOWNEY

Systems Programmer
University of Wyoming
Laramie, Wyoming
rowdydowney@gmail.com
Years in IT: II
Hobbies: Playing softball, fishing

Rowdy says that the Web-site–creation solution has saved the university's IT staff "countless hours" in the three years it's been in use. "We went from Web site requests taking a large chunk of time from multiple members of the IT team down to taking maybe one-quarter of a full-time employee's time. Much of the benefit is realized because site authors can manage their own sites without Help desk intervention. This saves a great deal of time on everyone's part and is much closer to a real-time solution." Although faculty and students as well as IT have benefited from the solution, Rowdy found that using his own resourcefulness and technical skills to solve the problem was equally gratifying. "This solution is an example of taking the tools you have available and molding them into the solution you need!"

Custom Logon-Tracking Solution

Keeping track of users' access to computers is an ongoing challenge for IT administrators. Brandon Jones, a systems administrator at Northern Arizona University—and two-time winner of a *Windows IT Pro* Innovators grand prize—faced this challenge by developing a custom logon-tracking solution that provides detailed information about students' computer use in the university's College of Business.

Brandon, who's one of four people in the business college's IT department, decided that the school needed a more efficient way to collect usage statistics for machines in different areas of the business-college building. Several factors led to his decision to develop the solution, ranging from a desire to know whether and when students used lab computers, to the ability to easily view logon data and track user statistics. "Microsoft tools such as event logs and user properties in Active Directory are cumbersome and don't even approach the level of detail and ease of use we were after," says Brandon.

The custom solution Brandon developed relies on disparate technologies, including VBScript scripts, Windows user environment variables, and Microsoft Access. Brandon explains how all these tools work together in his solution.

"When a user logs on to a machine in our domain, a Visual Basic logon script creates a new row in an Access database table, containing the username, computer name, and date/time of the logon. The script also creates a unique environment variable (the row number from the database table), which is stored on the local computer during that user's logon session. When the user logs off, a VBScript logoff script runs and, using the environment variable to look up the appropriate row in the database table, appends the logoff date/time for that user. The result is a single row (containing username, computer name, logon date/time, and logoff date/time) for every logon session that occurs in our domain."

With the logon information now housed in the database, Brandon can develop queries to specifically pull out needed information as requested. Information that can be drawn from the database includes logon and logoff times and session duration keyed by username. Using this information, Brandon has been able to provide faculty, at their request, with information about student activity. "A professor suspected that one of his students never showed up for an exam in a computer lab, even though the student insisted he had," says Brandon. "My solution not only confirmed that the student had logged on in the lab during the exam, but also told us the computer he used and how long he was logged on."

Brandon
JONES

Systems Administrator
Northern Arizona University
The W. A. Franke College of Business
Flagstaff, Arizona
brandon.jones@nau.edu
Years in IT: 7
Hobbies: Music, playing basketball, spending time with family

Brandon reports that the logon-tracking solution has been working effectively since implementation and that it also has had an unexpected side benefit: contributing to the arrest of a car thief. Thanks to Brandon's logon-tracking system, the university can provide

timely information to authorities when needed. "Last semester, information obtained from my solution helped police apprehend an individual who had stolen computers from one of our labs," says Brandon. "More recently, police arrested a car thief—who had logged on to one of our computers before taking someone's car keys—just hours after we provided them with information acquired from my solution."

To download Brandon's detailed explanation of his solution, go to www.windowsitpro.com, InstantDoc ID 97204, and click the Download the Code button.

Hands-Free, Large-Scale Software Deployment

Tim Manley oversees IT operations for a large overseas US Department of Defense installation. Until recently, Manley's IT staff spent an excessive amount of time keeping hundreds of computers at numerous remote sites updated. "Our legacy OS build was image based and required numerous man-hours to build or rebuild a PC," says Tim. "We had different images for each of our different makes and models—Windows 2000 ghost images that were sent out from headquarters, over a slow WAN link. Our guys might waste a whole day trying to find what image was supposed to go on which type of hardware." Compounding the problem was the fact that the upgrade process required a lot of manual tweaking and that systems frequently crashed because of outdated hardware.

Tim's challenge was to seamlessly automate the upgrade process so that his organization's planned migration to Windows XP and future upgrades could be done much more quickly and with minimal manual intervention. "I had just come on board, and my supervisor said, hey, we've got to automate this. The methodology we're using is so outdated and difficult to maintain, we need to look at other options." Because of tight security requirements, Tim's options for doing large-scale software upgrades were limited. "Basically, the only tool that I could find that would work in our environment was Remote Installation Services," he says.

Timothy
MANLEY

IT Specialist
US Department of Defense
manleyti@hotmail.com
Years in IT: 14
Hobbies: Fishing, travel, spending time with family

In less than a month, Tim developed a scripted RIS build process that he says enables "100 percent automated and hands-free OS and core application deployment." The build process is initiated on RIS servers at the organization's two main sites where IT staff rebuild machines; a build is replicated from one site to another to ensure an optimum transmission of the build over the WAN link.

When an IT staffer is preparing to replace a computer, he runs a premigration VBScript script to obtain configuration details about the computer to be replaced, such as what applications are installed, the computer's name, and its IP address. Finally, a postmigration script, which is part of the RIS automated installation, enables a variety of settings to ensure that the PC complies with government security requirements and other organization standards, such as the desktop background image and screen saver. "These are all settings that we couldn't do via Group Policy and didn't want to do manually," Tim says. "The goal was for the desktop guys to be able to hit the button and walk off. When they come back, they've got a complete OS build, and the user can then log on and use all their basic applications. Furthermore, since users' data is redirected to the user home drive via Group Policy, there's no data to migrate, and PCs can be rebuilt on the fly and swapped out without any loss of data or downtime to the user."

Tim's solution has made the upgrade process virtually painless for IT staff and much faster than before. "We've reduced migration time by 70 percent," says Tim. "Now it takes less than two hours from end to end to build a PC." Since completing the mass XP upgrade, IT staff have found additional uses for the automated build process. "About once a month we have to replace a machine, so we use the automated process for that," Tim says. Another key use is to slipstream software updates, such as service packs, applications, or new drivers, into a build, so that the update will be automatically included in future PC upgrades. "If we were still using an image-based upgrade process, the image might not be able to support the new hardware drivers. With RIS, we can just download and copy the drivers to the share, to immediately support new hardware."

RUNNERS UP

Intranet Portal Makeover

When he worked at Capitol Federal Savings, Ryan Rackley—now a senior local network administrator for ISG Technology—was spending an inordinate amount of time and money nursing a proprietary and crash-prone corporate intranet portal. Finally, he decided it was time for a change.

"The biggest problem was just how complex the system was," explains Ryan. "The portal application required software to be installed on each of our clients, as well as the server piece ... there were multiple points of failure in the system, and it was frequently down for days at a time." Ryan's headaches were amplified by inadequate support from the original developer of the system and an expensive service contract that was stretching department budgets. The time was right to make a switch, and Ryan decided that a better solution could be developed internally.

Ryan
RACKLEY

Senior Local Area Network Administrator,
ISG Technology
Topeka, Kansas
rrackley@cox.net

Ryan didn't have time to try a new standalone application, and the budget didn't allow for new servers or a new Microsoft SharePoint Portal Server installation. "We also wanted to keep the look and feel of our new solution as close as possible to the existing one," say Ryan. "We didn't want to confuse our users, so that consistency was important to us."

A small team of IT staffers began development of the new portal, which centered on using an open HTML format dedicating a file server to house company documents and other files accessed through the portal. Ryan's team eventually employed Adobe Dreamweaver to create the portal site, resulting in a more reliable solution that could be edited with off-the-shelf HTML editing tools. The new solution was created and deployed in a six-week timeframe and has since helped Capitol Federal realize substantial cost savings in its IT department budget.

All we are saying is give perfectly good hardware a chance.

VoIP is the future. So step into it. Not by ripping and replacing, but by sticking with the here and now. It's possible because now moving to VoIP isn't about hardware. It's about software. Keep your hardware—your PBX, gateways, even your phones. Move to VoIP with software. Software that integrates with Active Directory®, Microsoft® Office, Microsoft Exchange Server, and your PBX. Maximize your current PBX and phone investment and make it all part of your new software-based VoIP solution from Microsoft. Your hardware is ready when you are. Learn more at microsoft.com/voip

VOIP AS YOU ARE.

Your potential. Our passion.®

Microsoft®

"Our system uptime reached 100 percent after we switched, mainly due to the simplicity of the solution," says Ryan. Using Windows integrated security with AD eliminated the need for users to have multiple passwords, contributing to a 94 percent reduction in portal support calls when compared with the previous system. Ryan explains that for those reasons (and many more), the old system wasn't missed.

"We had used that system for more than two and a half years," says Ryan. "We had a big party when we unplugged that thing!"

Automating Imaging and Software Configuration

Regular upgrades and backups of the 120 tablet PCs in use at Midwest Palliative & Hospice CareCenter were becoming an increasingly onerous task, with one particularly nasty disk-imaging session finally convincing Jeff Ramsier, the center's network administrator, to find a more efficient solution.

"We had four people working on the upgrade—including me—and it still took us more than 12 hours to finish just the tablets," says Jeff. "[The] night we performed the install was at the end of a 30-hour day. We had to work on all 120-plus tablets with only seven power supplies … and half the batteries were almost dead." Jeff recounts how he and his support staff were forced to run from machine to machine, switching power supplies in order keep the laptops charged for the imaging process. "Once one of tablets goes down, the whole ghost imaging process stops until you get the [downed] tablet back up."

Determined to not go through a similar ordeal in the future, Jeff set to work on developing a series of Visual Basic scripts that could help automate some of the organization's most common administrative tasks. "For the most part, I did this all myself," says Jeff. "Microsoft's 'Hey, Scripting Guy!' Web site [www.microsoft.com/technet/scriptcenter/resources/qanda/default.mspx] helped with some of the VB scripting."

Jeffrey **RAMSIER**

Network Administrator, Midwest Palliative & Hospice CareCenter
Glenview, Illinois
j_ramsier@hotmail.com

Jeff's scripted solution helped automate many services, including installation of client software, printers, and faxes. It also configures installed software and synchronizes the laptop with the Misys medical software that the care center uses.

Now Jeff can easily image and update laptops as needed and has successfully transformed a time-consuming and error-prone process into a streamlined and efficient system. The new process requires only about 20 minutes for ghost imaging. Jeff likes the fact that he doesn't have to be present to perform installs and can install to and upgrade multiple tablets at the same time. "This solution is something that companies with a lot of tablets or laptops could use," he says. "Typically, in companies, the techs take a lot of time to image the tablets (or laptops), or they don't put much time into the image, so [the computer] isn't employee-friendly. This solution offers the best of both worlds."

Auditing Application Access for Compliance

In heavily regulated industries, some of IT's most crucial projects are bound to be driven by compliance mandates. That was the case for Michael Shire, who developed his winning solution in response to Canadian government regulations that require auditing a company's access to individuals' personal financial information. Michael's employer, a telecommunications firm, directed IT to track users' access to a payroll application (who, when, and how they gained access). Because access to the application is controlled through membership in AD security groups, Michael opted to fulfill the requirement by devising a way to monitor all AD-group modifications.

Michael initially looked into third-party products as potential solutions, but "there were no off-the-shelf packages that fulfilled the requirements for the project," he says. Michael has only moderate experience with scripting but, as he says, "I'm very good at solving puzzles, and I have a high Google IQ," so he relied mainly on his research skills to track down the components of the solution. "I pulled numerous sample scripts from the Microsoft Scripting Center and Google searches to accomplish everything required."

The solution Michael forged is basically a VBScript script using Windows Management Instrumentation to monitor all new events in the Windows security event log. Michael explains, "When an event related to a group modification occurs, the data from the event is written to a log. All AD group modifications are logged; however, monthly reports specific to the application are generated from this log in comma-separated value format. The script must run on all AD domain controllers (DCs) and keeps the logs and reports in a locked-down set of folders. The script is started as a service, where Windows can ensure that it's always running. Should the service stop, a warning message is written to the event log." The monthly reports are available to auditors upon request.

Michael **SHIRE**

Senior Network Administrator (Company name withheld by request)
Burlington, Ontario, Canada
mike_shire@hotmail.com

Michael's solution offers the additional advantage of being able to monitor all AD groups for other types of auditing. "I think the greatest benefit of the solution is its simplicity and scalability. If future AD groups require reporting, this can be easily accomplished by looking at the current reporting scripts. [The solution] can be applied to future DCs without rebooting them. Further, the code can be modified to look for other Windows event log entries, not just AD group modifications. You could call it Frankenstein's VBScript, but I find the results much more pleasant to live with!"

InstantDoc ID 97204

Anne Grubb

(agrubb@windowsitpro.com) is Web Lead Editor for *Windows IT Pro* and *SQL Server Magazine* and editor of *Exchange & Outlook Pro VIP*. She specializes in messaging and unified communications.

Jeff James

(jjames@windowsitpro.com) is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*. He specializes in virtualization and terminal services and has over 15 years of experience as a writer and digital-content producer.

PRINTER MANAGEMENT ESSENTIALS

BY ORIN THOMAS

Printer management is a crucial yet often annoying part of many IT pros' jobs. To keep things running smoothly, it's helpful to have a good background on the essentials of printer management. Let's look at how to share a printer, install extra drivers, use the Microsoft Management Console (MMC) Print Management Console (PMC) snap-in, troubleshoot, and do the myriad other tasks that contribute to your users' satisfaction and your job security. For consistency's sake, we'll assume you're logged on to Windows Server 2003 with an account that has administrator permissions.

Get the basics on printer sharing, pools, permissions, and troubleshooting, and keep your users happy

Sharing a Printer

After a printer is connected to a Windows 2003 computer and you verify that it works using a print test page, you can share the printer. To share a printer, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the printer, and select Properties.
2. Click the Sharing tab, then select the *Share this Printer* radio button.
3. Enter the printer's shared name. You should try to name your printers according to a convention that is easily understood. A convention that incorporates location and function is recommended. Ensure that the *List in the directory* check box is selected.
4. Click OK to close the dialog box.
5. Right-click the printer again and select Rename.
6. Enter the same name that you entered in the shared name dialog box.

Always remember that a printer's shared name isn't the same as the name listed in AD, even though the dialog box gives the impression that this is the case. The AD listing is based on the name the printer is assigned in the host Windows 2003 computer's Printers and Faxes folder. If you can't find a recently shared printer within the directory, check what name is assigned to the printer in Printers and Faxes. You should attempt to ensure that these names match to avoid confusion.

ILLUSTRATION BY ALEXANDER BARSKY / IMAGES.COM

Figure 1: Installing extra print drivers

Installing Extra Print Drivers

Unless already installed, a client computer will obtain and install the necessary drivers when it first connects to a shared printer. Microsoft calls this technology "Point and Print." In general, a printer driver installed on a Windows 2003 computer will work with Windows XP and Windows 2000 Professional computers. Where you must be careful is when you have a mix of computers with 32- and 64-bit processors. If your print server's processor architecture differs from some or all of your print clients (e.g., x64 as opposed to 32-bit), you must manually install drivers for the alternative architecture when you configure the shared printer. To do this, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the printer, and select Properties.

2. On the Sharing tab, click Additional Drivers.

3. Select the check box next to the additional driver you want to install, such as x64, as Figure 1 shows, and click OK.

4. Enter the path to the additional driver software and click OK. You should ensure that printer drivers are installed on the print server so that user's aren't prompted for drivers on their workstations.

It's not possible to install Windows Vista-specific drivers in this manner. Usually this won't be a problem because Windows 2003 and XP client printers generally work with Vista clients. However, in some cases, drivers that work for XP and Windows 2003 don't work on Vista because of Vista's tighter security. If no compatible driver exists on the Windows 2003 print server, Vista will check its own driver store. If a Vista-compatible driver already exists on the Vista client computer, this driver will automatically be used. If no such driver is included with Vista, you'll need to install an updated driver on the Vista client computer. You can do so manually or by deploying the printer to the Vista client through AD, which I cover later in this article.

Managing Printers

Although I recommend you use the PMC snap-in to manage printers, the management tool that most administrators are used to is the Control Panel Printers and Faxes applet in Windows 2003 and XP. This applet provides a list of printers installed on the computer, the number of documents in the queue, and the status of the printer. Double-clicking a printer in the Printers and Faxes applet shows you the shared printer's queue. The printer queue provides you with information about who submitted the document, how large it is, and when it was submitted. You can view two important menus in the print queue:

- The Printer menu lets you pause all print jobs, cancel all print jobs, and configure the printer to be used offline.
- The Document menu, which you access by selecting a document in the queue, lets you pause the document, resume the document, cancel the print job, and restart the print job from the beginning.

Print Management Console. The best tool for managing printers is the PMC snap-in, which is available in Windows 2003 R2 when you add the Print Server role. It's not presently available for Windows 2003 SP1. The primary benefit of PMC over previous methods of printer management is that it lets an administrator view and manage all printers in an organization, as Figure 2 shows, not just those connected to the local print server. PMC can monitor shared printers attached to Windows 2003 R2, Windows 2003, and Win2K Server print servers.

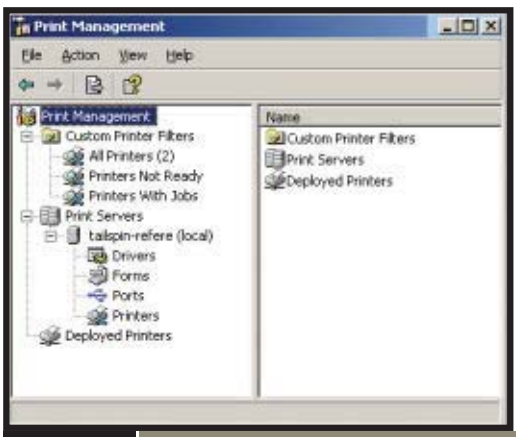


Figure 2: Print Management Console interface

Perhaps the most useful aspect of PMC is the Custom Printer Filters node, which lets an administrator view printers in the organization that aren't ready due to an error and that require attention. At this node, you can also create individual custom filters and configure them to show only shared printers with a specific number of print jobs, which you could use to identify heavily used printers. You can also configure filters to send email alerts to administrators when specified conditions, such as a paper jam, occur. Email alerts can be configured only with created filters and can't be applied to the console's default filters.

Command line. Command-line printer management options let you automate certain printer management functions through scripting. Command-line printer management programs and scripts are located in the \%systemroot%\system32 directory. The most useful printer management scripts are the following:

- prnjobs.vbs—can be used to view and manage print jobs
- prncfg.vbs—allows shared printers to be modified
- prnqctl.vbs—allows management of a printer's queue

You can use these scripts to manage remote printers as well as printers attached to the computer on which they are run. You could also specify alternative credentials with each of these scripts. A properly configured batch file could be used to pause all printers in a domain or purge their print queues. For more information about these command-line options, see the Microsoft article "New Command-Line Tools" at technet2.microsoft.com/windowsserver/en/library/4c475b4c-e5ee-444c-a730-ccb7a13e03b41033.mspx?mfr=true.

Configuring Printer Pools

A bottleneck for some organizations is the speed at which printer hardware outputs pages. Adding a second or a third shared printer often doesn't work as a solution because it's difficult to balance users' output manually. The solution is printer pools, which balance output across multiple print devices.

30 million computer users don't trust the power grid.

APC **Smart-UPS® 1000** provides power protection and battery backup during power outages.
Also available in rack-mount models.

They do trust APC. Shouldn't you?

"Overall the reliability of electrical systems in the US almost certainly will decline over the next 10 years."

– Venture Development

Think of all that you rely on your computer for: personal and business files, financial information, broadband access, videos, photos, music, and more

Increasingly, computers are the hub for managing our lives. And more people rely on APC to protect their hardware and data than any other uninterruptible power supply (UPS) brand.

Why is APC the world's best selling power protection? For 20 years, we have pioneered power protection technology. Our Legendary Reliability® enables you to save your data, protect your hardware, and prevent downtime. It also guards against a power grid that is growing less reliable every day.

According to the Department of Energy, electricity consumption will increase by 40% over the next 10 years. Yet today, investment in utilities is at an all-time low. It's a "perfect storm" for computer users, one that makes APC protection even more essential.

APC has a complete line of power protection solutions to suit a range of applications. Already an APC user? Get the latest replacement battery cartridge for your unit or upgrade to a newer model.

Find out why 30 million people don't need to worry about losing their music, photos, and financial files.

Find APC power protection products at: COMPUSA We got it. We get it. CDW Office DEPOT

APC Solutions for Every Level of Protection

Home Starting at $59.99
Best value battery backup and surge protection for home computers.
8 outlets, DSL protection, 44 minutes of runtime

Back-UPS® ES 550R

Home Office Starting at $99.99
Complete protection for home and small business computers.
10 outlets, DSL and coax protection, 70 minutes of runtime

Back-UPS® ES 750

Small Business Starting at $459.00
High-performance network power protection with best-in-class manageability for servers.

Smart-UPS® 1000

Register to WIN a Smart-UPS® 1000 – value $459 ERP.

Also, enter keycode to view other special offers and discounts.

APC® Legendary Reliability®

Visit www.apc.com/promo and enter key code x610x • **Call** 888-289-APCC x4671 • **Fax** 401-788-2797

e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • BK1A7EF-EN

With a printer pool, users send jobs to a single shared printer, and that printer allocates the job to the next available hardware device in the pool. The primary limitation of printer pools is that the driver used must be compatible with all printer hardware in the pool. Generally this means that you should use identical printer hardware for each device in the pool, but you can get away with using a basic printer driver that's compatible with many models of printers as long as your users don't require many printing features.

The devices used in a printer pool should be located in the same area, as users aren't notified which specific device has printed their jobs. If you set up a printer pool with identical devices on the first, second, and third floors of a building, users might have to check all three locations to find their jobs. To configure a printer pool on an existing shared printer, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the shared printer you want to pool, and select Properties.

2. On the Ports tab, select the *Enable printer pooling* check box.

3. Click Add Port to add a new port. Configure this port to connect to an extra hardware device.

4. Keep adding ports until all print devices in the pool are added to the shared printer.

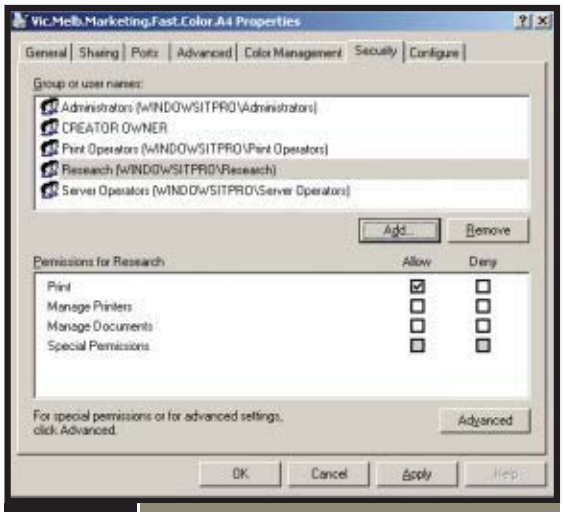


Figure 3: Shared printer security permissions

Setting Printer Permissions

By default, all users in a domain are able to print to a shared printer. Often you will want to configure printers so that only particular groups can print to specific printers. For example, it might be necessary to ensure that only the CEO and his or her administrative assistant can print to the shared printer in the assistant's office. Three basic print permissions are available for each shared printer:

- Print—This permission allows the user or group granted it to print to the shared printer.
- Manage Printers—This permission allows the user or group granted it to modify shared printer properties, including print permissions.
- Manage Documents—Users or groups granted this permission can pause, restart, or delete any documents in the printer queue, regardless of who owns them. By default, users have the Manage Documents permission on their own print jobs.

To configure permissions on a shared printer, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the printer, and select Properties.

2. Click the Security tab, which Figure 3 shows. Under *Group or user names*, remove the Everyone group from the list by selecting it and clicking Remove.

3. Click Add to add the group or users that will have permission to print to the shared printer.

Setting Print Priority

Multiple shared printers can be configured to use a single print device. By assigning each shared printer a different priority and configuring separate permissions on those shared printers, it's possible to let one group jump the queue and print their documents before another group. The default priority of a shared printer is set to the lowest possible value, which is 1. The highest possible priority value is 99.

If there are five jobs with a priority of 1 in the queue and a job with a priority of 99 is submitted, the job with the priority of 99 will be bumped to the top of the queue but won't displace the job currently being output on the print device even if it's of a lower priority.

To configure a printer's priority, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the printer, and select Properties.

2. Click the Advanced tab and adjust the number in the Priority box to the appropriate setting.

3. To ensure that the group that should have its documents printed most quickly is the only one allowed to use the shared printer, configure security appropriately as I covered in the previous steps.

The most common mistake in configuring print priorities is to assume that a lower assigned priority number means documents will print faster. Ensure that the shared printer you configure for your organization's executives has a higher priority than the one you configure for ordinary users.

Troubleshooting PRINTER PROBLEMS

Printer problems are generally caused by a document that has a problem or by the print spooler failing. It can sometimes be difficult to determine if the problem is a document or the shared printer as a whole. Your first attempt at troubleshooting should be to deal with the document. If that fails to solve the problem, you should look at the shared printer. To troubleshoot printer problems, do the following:

1. If a document has failed, first try to restart the job.

2. If restarting the document doesn't work, attempt to delete the document from the queue.

3. If you're unable to delete the document from the queue or unable to restart the job, you'll need to restart the spooler service. The quickest way to do this is to open the Print Spooler service on the Print Server using the Services console. Right-click the Print Spooler and select Restart.

InstantDoc ID 97148

Managing Print Queues

Some users repeatedly print out very large jobs, blocking printer access to everyone else until their job is complete. Using a combination of security settings and printer availability settings, it's possible to ensure that these jobs are output only during specific times.

When a job is submitted to a shared printer that has particular availability settings, the print server holds the job until the printer becomes available and then outputs it. Printer availability allows big jobs to be submitted to a shared printer during office hours and output in the middle of the night. As the job is spooled on the print server, the client computer from which the job was submitted can be switched off when the person who uses it leaves for the evening. Figure 4 shows printer availability settings. To configure the times at which a shared printer is available, perform the following steps:

1. Start the Control Panel Printers and Faxes applet, right-click the printer, and select Properties.

2. On the Advanced tab, select the *Available from* option and configure the hours when the printer will be active.

3. Instruct users who are printing large, non-urgent jobs to submit to this shared printer instead so their jobs can be output during slower periods.

Figure 4: Printer availability settings

Publishing Printers via AD

If a domain is upgraded so that it has Windows 2003 R2 domain controllers (DCs), it's possible to use AD to publish specific printers to users and computers that fall under the influence of a specific Group Policy Object (GPO). PMC, available with R2 and covered earlier in this article, vastly simplifies the process of deploying printers via AD. To deploy via Group Policy, an existing GPO must have been created and linked to an appropriate site, organizational unit (OU), or to the domain. To deploy a printer via AD using PMC, perform the following steps:

1. Open PMC.

2. Either in the All Printers node under Custom Printer Filters, or in the Printers node under a specific print server, locate the printer you want to use AD to deploy.

3. Right-click the printer and select *Deploy with Group Policy*.

4. In the *Deploy with Group Policy* dialog box, which Figure 5 shows, click Browse. Locate the target GPO and click OK.

5. Depending on whether the printer is to be deployed on a per-user and/or a per-computer basis, select the appropriate check box, then click Add.

6. Any existing printers that have been deployed using that GPO will be listed in the table. To remove these printers, select them and click Remove.

7. When you're satisfied with the list of deployed printers, click OK.

8. The Deployed Printers node, at the bottom of the PMC screen, will now display the newly deployed printer.

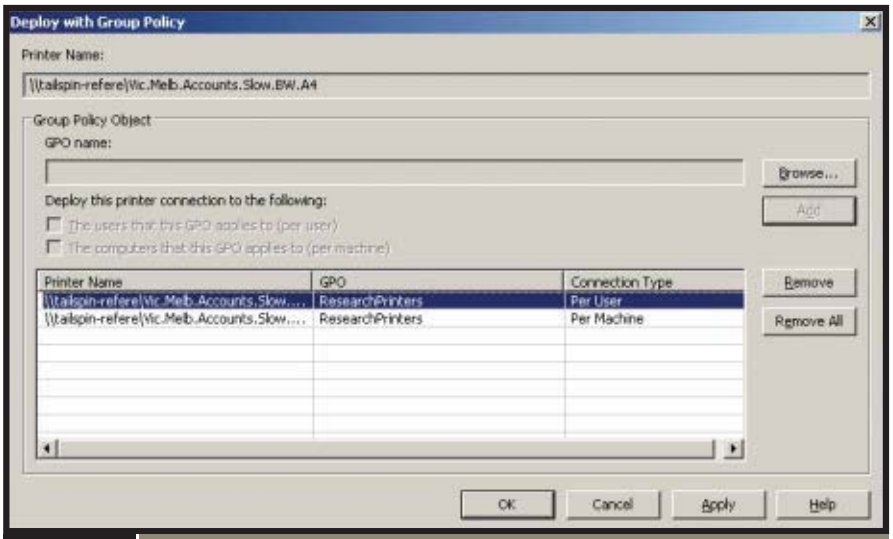


Figure 5: *Deploy with Group Policy* dialog box

Remember the Basics

No matter how careful you are in managing your printers, things can still go wrong. Some quick troubleshooting hints are listed in the sidebar "Troubleshooting Printer Problems," page 42. Printer management is a daily task that almost all systems administrators deal with. Armed with the print management tools and options available in Windows 2003 R2, and this refresher, I hope you'll find this task goes smoothly.

InstantDoc ID 97147

Orin Thomas

(orin@windowsitpro.com) is a contributing editor for *Windows IT Pro*, a Windows Security MVP, and has authored or coauthored more than a dozen books for Microsoft Press.

Extending Virtual PC with Virtual Server

Take your virtualization endeavors to the next level

by Desmond Lee

In a recent project, I helped build a self-contained virtualized infrastructure based on a couple of virtual machines (VMs) with AD, DHCP, DNS, RIS, and WINS services running on them. The team started with Microsoft Virtual PC 2007 and installed the latest Virtual Machine Additions. (To learn about the often-overlooked task of installing Virtual Machine Additions, see the Web-exclusive sidebar "Essential Virtual Machine Additions, InstantDoc ID 97288.) After placing the solution in production for a while, we saw that the VM infrastructure just couldn't cope with the load that our project demanded. To solve the problem, we ultimately installed Microsoft Virtual Server 2005 SP1, and ported the VMs over by making the necessary modifications and attaching the VHDs to SCSI adapters.

Virtual PC is an excellent, inexpensive tool for building precinct environments, whether for Help desk support or for testing security patches before production rollout. But as your needs grow, you might encounter similar limitations in performance and scalability. Or perhaps you've already built a core library of VMs and would like to reuse them in a secured server-farm environment.

Virtual Server might just be the answer you're seeking. Microsoft's well-designed virtualization architecture permits an almost seamless integration and interoperability between Virtual PC and Virtual Server. After a couple of free downloads, and a little tinkering, you'll be able to tackle any virtual environment.

VM Architecture

For information about how to download both Virtual Server and Virtual PC for free, see the Learning Path. Before you start your download, however, you need to understand the subtle differences between Virtual PC 2007 and Virtual Server 2005 to help make porting VMs between the two platforms a little less painful. For the purpose of this article, all references are to Virtual Server 2005 R2 SP1 Enterprise Edition and Virtual PC 2007. Discussions about Virtual PC 2007 also apply to Virtual PC 2004 SP1, unless otherwise stated.

The design philosophies of Virtual PC and Virtual Server differ in their purpose and market segments. Put simply, Virtual PC targets the average desktop user, focusing on tight host-guest integration, ease of use, and a rich user experience. Virtual Server, by contrast, is aimed toward the enterprise-server sector, in which buzzwords such as manageability, scalability, and security are paramount.

Even considering this market distinction, you'll find that Virtual PC and Virtual Server share a fundamental set of core features. The key enabler that facilitates VM porting between the platforms is the common file architecture: the virtual machine configuration (VMC) file and the virtual hard disk (VHD). The VMC file is an XML configuration file that contains metadata describing the VM. The actual disk storage as seen by the VM is enclosed in one or more VHDs.

The system automatically creates virtual machine saved state (VSV) files and undo disk (VUD) files, if enabled, in the same folder in which the VM is defined. The VSV file stores the suspended state of a running VM for restoration at a later time. The system writes changes made while a VM is in use to the VUD file, where rollback to a good known state can be accomplished by discarding the changes instead of committing them to disk. VSV files are incompatible between the two platforms. Hence, to avoid potential problems, modifications should always be flushed to disk and the VM properly shut down before moving VMs between Virtual PC and Virtual Server. The virtual network configuration (VNC) file is unique to Virtual Server and isn't used under Virtual PC.

Figure 1: Inspecting the VHD before importing

The Basics

Moving a Virtual PC–built VM to Virtual Server is as simple as accessing Virtual Server's administration Web site and specifying the fully qualified path of the VMC file under Virtual Machines, Add. I do recommend that you first use the Virtual Disk, Inspect option. Doing so

```
<ethernet_adapter>
  <controller_count type="integer">1</controller_count>
          <ethernet_controller id="0">
                    <virtual_network>
                              <id type="bytes">00000000000000000000000000000000</id>
                              <name type="string"> Intel(R) PRO/1000 Connection</name>
                    </virtual_network>
                    <id type="integer">0</id>
                    <ethernet_card_address type="bytes">000000000000
                              </ethernet_card_address>
                    <is_dynamic_assignment type="boolean">true
                              </is_dynamic_assignment>
          </ethernet_controller>
</ethernet_adapter>
```

Figure 2: VMC network settings

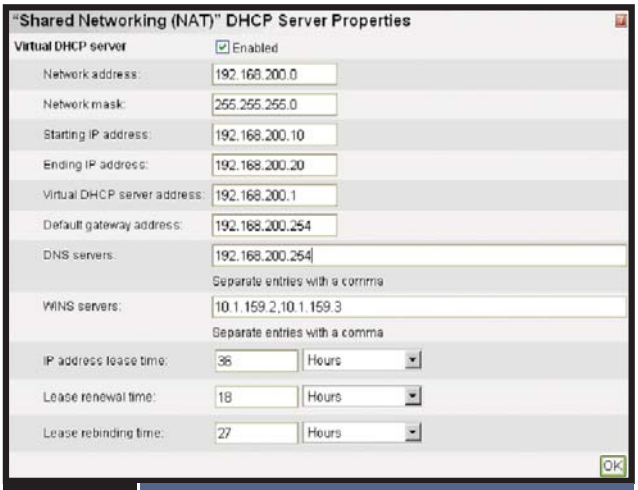


Figure 3: User-defined DHCP settings in Virtual Server

helps to verify the integrity of the VHD, including any dependency, such as the case when the VHD is set up as a differencing disk linked to its parent, as Figure 1, page 45, shows.

You might have a need to port a VM in the reverse direction, from Virtual Server to Virtual PC—for example, when the target machine doesn't have Virtual Server installed or you want to enable some Virtual PC–specific features. To do so, open the Virtual PC console and start the New Virtual Machine Wizard. Select *Add an existing virtual machine* and point to the fully qualified path of the VMC.

As you can see, deploying an existing VM on either platform is as straightforward as adding the VM itself. Nevertheless, a few device types and functionalities will behave differently due to architectural variation between the products. Web Table 1 (InstantDoc ID 97084) outlines some potential interoperability problems.

Networking Details

Both Virtual PC and Virtual Server support a maximum of four virtual network adapters per VM. Although the internal VMC file structure is common, networking is one aspect that differs slightly on the two platforms. Virtual PC stores network-configuration information directly in the VMC file with the same name as the VM, under the ethernet_adapter section, which Figure 2, page 45, shows.

The actual description of host network adapters available to a user resides in the options.xml file, which resides at %APPDATA%\Microsoft\Virtual PC. Because Virtual PC has no GUI front end for changing the network adapter name, you'll have to modify <name type="string">*Manufacturer Network Adapter Name*</name> in the <virtual_network id="n"> section. Remember to make a backup copy of the file before editing it.

Virtual Server stores network settings in separate XML configuration files with a VNC extension. You'll find them under %ALLUSERSPROFILE%\Documents\Shared Virtual Networks, and only local administrators have access to this folder in a standard installation. By default, the system creates a number of files that match the physical network adapters present on the host. Suppose you have two internal network adapters, one wired and the other wireless. Virtual Server will create two files named External Network (*manufacturer name and wired NIC model*).vnc and External Network (*manufacturer name and wireless NIC model*).vnc. Additionally, Internal Network .vnc is also automatically created to facilitate VM-to-VM communication only.

Virtual Server lets you create an infinite number of virtual networks, each with a fully customizable virtual DHCP Server, as you see in Figure 3. There's also no limit to the number of VMs that can connect to each virtual network. By separating VNC files that describe various common network settings, you achieve isolation without tying a physical network adapter to a specific VM or user.

Obviously, performance will suffer if you attach multiple network-intensive VMs to the same virtual network, which is typically associated with a physical network adapter on the host. The trick is to install multiple adapters on the host and distribute the load among the pool of VMs, according to usage and application needs.

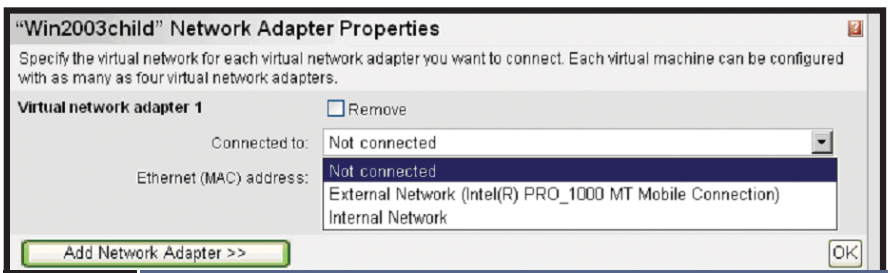


Figure 4: Binding to a virtual network in Virtual Server

Listing 1: Simple Script to Bind to a Virtual Network Under Virtual Server

```
Set objVS = CreateObject("VirtualServer.Application")
Set objVM = objVS.FindVirtualMachine("name_VM")
Set objVN = objVS.VirtualNetworks

Set countNICs = objVM.NetworkAdapters

'assumes only a single Virtual Network Adapter is attached to the VM
'attaches to the first available physical network adapter (host OS) listed
countNICs(1).AttachToVirtualNetwork objVN.Item(1)

Set objVS = Nothing
Set objVM = Nothing
Set objVN = Nothing
```

Learning Path

WINDOWS IT PRO RESOURCES

"Server Virtualization Basics," InstantDoc ID 50236

"Windows Server Virtualization Features," InstantDoc ID 96261

"What You Need to Know About The Virtualization Format War," InstantDoc ID 92862

MICROSOFT RESOURCES

Download Virtual Server 2005 R2 SP1 Enterprise Edition for Free

www.microsoft.com/technet/virtualserver/software/default.mspx

Download Virtual PC 2007 for Free

https://www.microsoft.com/downloads/details.aspx?familyid=04D26402-3199-48A3-AFA2-2DC0B40A73B6

Installing Virtual Machine Additions

www.microsoft.com/technet/prodtechnol/virtualserver/2005/proddocs/vs_deploy_setup_VM_OS_additions.mspx

Virtual PC vs. Virtual Server: Comparing Features and Uses

www.microsoft.com/windowsserversystem/virtualserver/techinfo/vsvsvpc.mspx

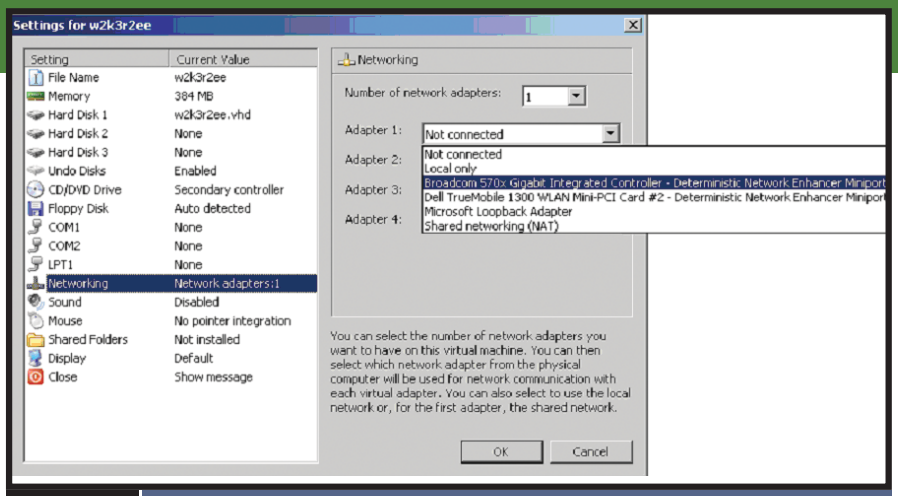


Figure 5: Manually attaching the VHD and network adapter in Virtual PC

Because of this subtle difference in virtual network configuration, moving a Virtual PC–created VM already configured with networking to Virtual Server (or vice versa) might result in an error, leaving the network adapter in an unplugged, unconnected state.

To connect to a virtual network under Virtual Server after importing a VM from Virtual PC, click Network Adapters, then OK after selecting the correct connection, as you see in Figure 4. Network connectivity will be available once the guest OS is started, without further configuration necessary.

Unfortunately, you must perform this manual process every time you move a VM from Virtual PC to Virtual Server. However, the reverse isn't true. Alternatively, you can use a script such the one in Listing 1 to automate this task.

Putting It to Work

Now, let's put everything into practice. In our sample scenario, we have a VM originally created with Virtual Server. We're porting from Virtual Server to Virtual PC to take advantage of the new hardware-assisted virtualization support that's available only in Virtual PC 2007. This also demonstrates the important fact that the VHD file structure is generic and can be attached to a different adapter type (SCSI or IDE).

1. Ensure that the guest OS is properly shut down under Virtual Server.

2. Make a backup copy of the XML-based VMC file.

3. Start Virtual PC and walk through the New Virtual PC Wizard.

4. Select the *Add an existing virtual machine* option, and specify the full path of the existing VMC.

5. Inspect the VM settings, and notice that Hard Disk 1 and Adapter 1 appear as None and Not Connected, respectively, as Figure 5 shows. Before you attempt to start the VM, you must manually define a hard disk by attaching to the previously created VHD. If network connectivity is desired, you must explicitly connect a physical network adapter as well.

6. You're now ready to start the VM. Highlight the VM in the Virtual PC Console, and click Start. Immediately, you'll see warnings about incompatible hardware settings. You can safely ignore these warnings by clicking OK.

7. If you've explicitly selected the *Enable sound card* option in the VM settings, Plug and Play (PnP) will kick in automatically and you'll be prompted to install the appropriate sound drivers in the guest OS. A reboot might be necessary, after which you can use the VM without further modifications.

Dive In

Return of Investment (ROI) is key in today's fast-paced and competitive landscape. Virtualization can let you ensure the timely support and coexistence of legacy applications, as well as handle the onslaught of new technologies. IT investments in Virtual PC technology can easily be expanded to a larger scale when your organization is ready to move up. The good news is that you can accomplish this ideal scenario without sacrificing compatibility or throwing money at costly retraining. All you have to do is dive into Virtual Server's enterprise-class features.

InstantDoc ID 97084

Desmond Lee

is a senior consultant at BT Global Professional Services (Switzerland). He is a Microsoft Certified Trainer, a technology evangelist, and founder of the Swiss IT Pro User Group (www.swissitpro.ch). You can read his blog at www.leedesmond.com/weblog.

Statement of Ownership

Statement of Ownership Management and Circulation for *Windows IT Pro* magazine as required by 39 U.S.C. 3685; *Windows IT Pro* magazine, publication no. 1552-3136, filed October 1, 2007, to publish twelve monthly issues each year for an annual subscription price of $49.95. The mailing address of the office of publication, the headquarters of general business of Kim Paulsen, Group Publisher, and Karen Forster, Editorial and Strategy Director, is 221 E. 29th St., Loveland, CO 80538. The owner is Penton Media Inc., 249 W. 17th St., 4th Floor, New York, NY 10011-5390. Penton Business Media Holdings, Inc., of 249 W. 17th St., 4th Floor, New York, NY 10011-5390 owns 100% stock in Penton Media, Inc. The average number of copies of each issue published during the twelve months preceding the filing date include: total number of copies (99,224); paid mail subscriptions (57,267); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (11,287); paid distribution through other classes of USPS mail (323); total paid circulation (68,877); free or nominal rate distribution by mail (21,968); free or nominal rate distribution outside the mail (4,234); total distribution (95,079); copies not distributed (4,145) for a total of (99,224) copies. The actual number of copies of single issues published nearest to the filing date include: total number of copies (92,306); paid mail subscriptions (51,157); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (13,600); paid distribution through other classes of USPS mail (323); total paid circulation (65,080); free or nominal rate distribution by mail (23,612); free or nominal rate distribution outside the mail (1,898) total distribution (90,590); copies not distributed (1,716) for a total of (92,306) copies.

I certify that the statements made by me above are correct and complete:

—Kim Paulsen, Group Publisher.

NETWORK ACCESS PROTECTION IN WINDOWS SERVER 2008

by Damir Dizdarevic

Using NAP to Verify a Computer's Health Before Allowing Network Access

1 Prepare the environment: Install DHCP on a Windows Server 2008 DC with AD enabled, and add the Network Policy Server and DHCP Server roles.

2 Configure health policies (i.e., the System Health Validator and Health Policy options).

3 Create network policies for NAP: Configure policies for incompliant and compliant clients, as well as a policy for NAP non-capable clients.

4 Configure DHCP for NAP: Configure the DHCP server to distribute a different group of scope options to compliant and incompliant NAP clients.

5 Enforce NAP on the client side: Use the NAP Client console, Group Policy, or Netsh to configure the client to work with NAP.

[**Editor's Note:** This article is based on Windows Server 2008, post-Beta 3 June Community Technology Preview (CTP) build, which was the version available at article submission time. Note that some of the options and screens might change in the final release.]

In considering LAN security, we mostly think about preventing an attacker from accessing network resources. The reason for this focus is simple: Most attacks are initiated from the Internet and are directed at breaking into private networks.

However, an equally large security issue that administrators must address is preventing regular (i.e., authenticated and authorized) network users from using computers with weak security configurations to access network resources. For example, a traveling employee might have a laptop that only occasionally uses the VPN to connect to the corporate LAN—but this laptop still needs all the current security fixes, antispyware, and antivirus definitions installed. Otherwise, such a computer is a likely source to spread viruses or worms on the network. If a computer doesn't have a firewall enabled and becomes infected with Trojan-like software, the computer can provide unauthorized persons with easy access to local network resources. Employees' home computers that use the VPN to access the corporate LAN and that aren't managed properly provide a similar risk. Finally, letting visitors connect their computers to your local network, even just to provide them with Internet access, can put other hosts on the network at risk for infection with viruses or other kinds of malicious code.

The question is: How do you check a computer's security configuration before you allow it to access network resources? In addition, how do you determine whether to grant full or limited access? Network administrators need a mechanism to ensure that any computer connecting to the corporate network meets the organization's health policy requirements and has all the necessary software, patches, and hotfixes installed.

Network Access Protection

Windows Server 2003 SP1 includes a technology called Network Access Quarantine (NAQ) that helps administrators limit or deny connections to computers that don't comply with a company's security policies. However, NAQ has many disadvantages. First, it's limited to VPN-based connections only, which means you can't protect your network from unsecured wireless users, or even from users who have a physical connection to the network (e.g., via employees' personal laptops). Second, NAQ is based on manually created scripts (implemented via Connection Manager) that must be run on the client side before VPN access is granted. These scripts check such things as the firewall state, antivirus state, presence of a password-protected screen saver, and status of Internet Connection Sharing. Besides the fact that writing the scripts can be difficult and time consuming, the various types of protection software on the client side can also cause problems. For example, if VPN clients have various antivirus programs, you must write a specific script for each program and use a different Connection Manager package for each. In the end, this solution is static. After the client passes all the checks and the main script reports the state of the client's health to the server, the user can safely disable the firewall, antivirus software, and all other security features. These actions won't be detected, and the level of access to resources will remain unchanged.

Windows Server 2008 solves most of NAQ's disadvantages with Network Access Protection (NAP) technology. Using NAP, an administrator can enforce specific compliance policies that must be met before a client computer can access network resources. If a client computer doesn't meet the defined health requirements, it's either placed in quarantine (with access

Verify computers' security before allowing network access

limited to specific hosts) or simply not allowed access.

In addition, NAP can automatically remediate unhealthy clients, updating systems when possible to make them comply with corporate policy. The administrator configures NAP's method of enforcement, depending on the type of client connection. NAP enforces health requirements for the following types of connections:

- IPsec-protected communications
- IEEE 802.1x-authenticated connections
- VPN connections
- DHCP-managed connections
- Terminal Services Gateway connections

In this article, I focus on NAP implementation for DHCP-managed connections. Using NAP with DHCP lets you protect your network from all potentially unsecured clients that are managed via DHCP (i.e., clients that receive IP addresses from DHCP), including resident desktop computers that are NAP capable.

NAP-capable OSs include Windows Vista (by default) and Windows XP SP2 with NAP client software (currently in Beta 3). XP SP3 will include the NAP client by default. No older OSs are supported, because NAP relies on information from Windows Security Center (WSC), which exists only in Vista and XP SP2.

A benefit of NAP is that it's not limited to Microsoft technologies. Any system that can provide the NAP server with its health state can also use NAP. Microsoft is working with many hardware and software vendors and other partner companies to help them create NAP-compatible devices and software. To use NAP for DHCP-managed connections, you must prepare the environment, configure health policies, create network policies for NAP, configure DHCP for NAP, and enforce NAP on the client side.

Prepare the Environment

First, you must have an existing Active Directory (AD) infrastructure available, with one or more Windows 2003-based (or Server 2008-based) DCs. DHCP must be installed on a Server 2008 machine, because previous versions of the DHCP service (such as the version on Windows 2003) aren't aware of NAP. You need at least one static IP address for this host.

Install Server 2008 as a member server in your domain. After installation, you must add the Server 2008 roles called Network Policy Server and DHCP Server. You can easily accomplish this task through the Server Manager console, which is available on the Welcome page or under Administrative Tools. Open Server Manager, go to Roles Summary, and click Add Roles. Server 2008's Network Policy Server role replaces Windows 2003's Internet Authentication Service (IAS). Thus, Network Policy Server (NPS) lets you create various types of policies, not just those related to NAP.

Configure Health Policies

To configure your health policies, go to Administrative Tools and click the Network Policy Server role you added. In the NPS console that opens, you must configure the System Health Validator and Health Policy options to create an appropriate network policy. The System Health Validator component defines your security requirements for clients that are accessing the network, whereas Health Policy defines different configurations for NAP-capable clients.

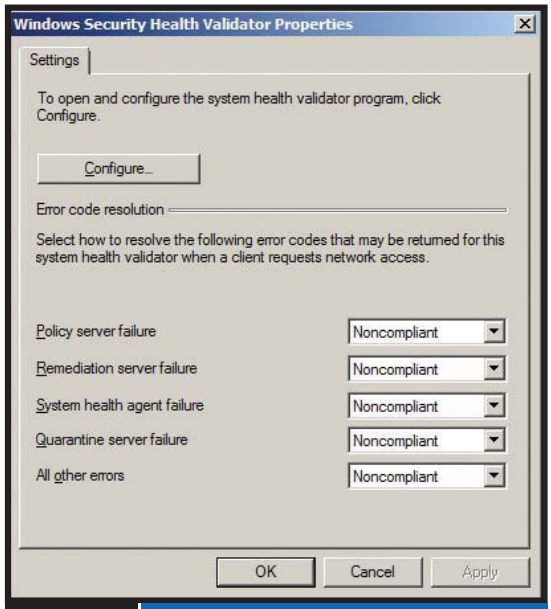


Figure 1: Configuring Windows Security Health Validator properties

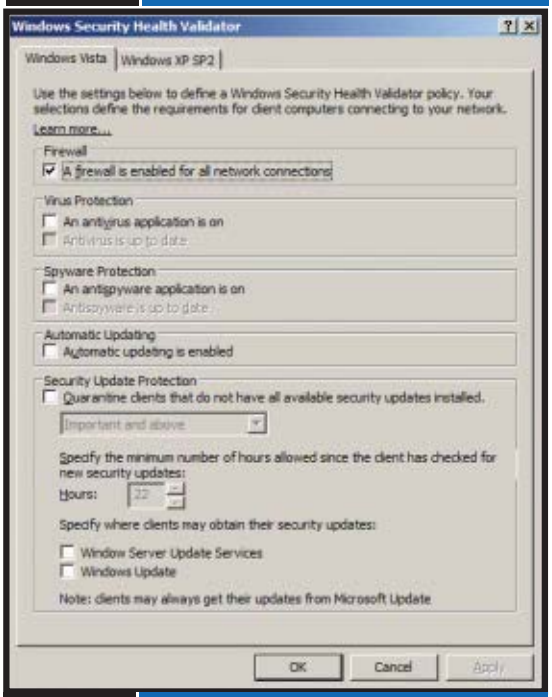


Figure 2: Setting security requirements for Windows Vista clients

Double-click the Network Access Protection node on the left side of the console, and click System Health Validator. The Windows Security Health Validator item will appear on the right side of the console. Double-click this item to open the configuration window that Figure 1 shows. In this window, click Configure to see options for security requirements. As Figure 2

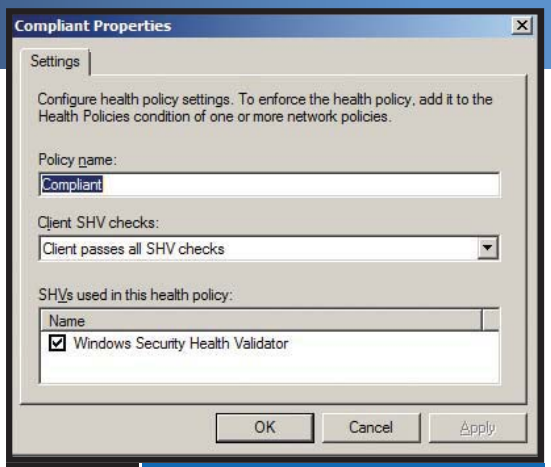


Figure 3: Configuring the Health Policy option

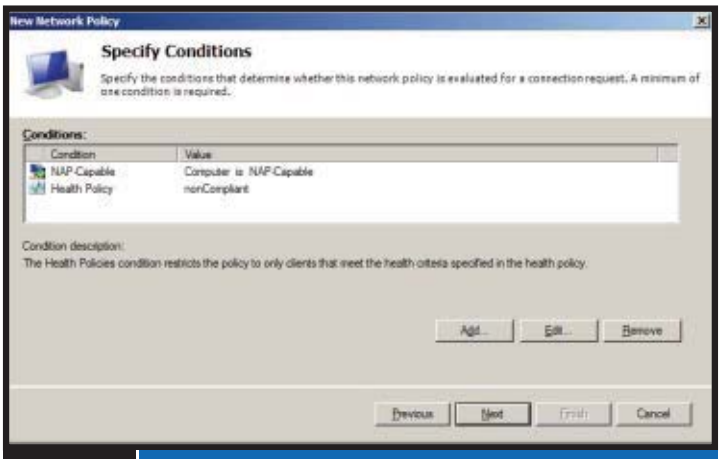


Figure 4: Adding the NAP-Capable condition

shows, you can simply select the appropriate check boxes to indicate what you require from clients. In Vista, you can require the firewall to be enabled, antivirus and antispyware applications to be present and current, the automatic update feature to be enabled, and current hotfixes to be installed. Similar requirements are available in XP SP2, other than the antispyware option, which isn't part of XP. For testing purposes, let's select only the firewall check box for both Vista and XP. Click OK twice to finish configuring the System Health Validator option.

To configure the Health Policy option, double-click the Policies node in the NPS console, right-click Health Policies, and select New. In the window that Figure 3 shows, enter the policy name and select what the System Health Validator (SHV) component will check.

First, let's create a policy for compliant clients. Enter *compliant* for the policy name, and select *Client passes all SHV checks* from the drop-down menu. Selecting this option means that, for a client to be considered healthy, it must pass all the requirements you configured in SHV (which in the example was only the firewall requirement). Next, select the Windows Security Health Validator check box and click OK. Your first policy is now configured.

Next, let's create a policy for noncompliant computers. Follow the same steps to create a new health policy, perhaps called *noncompliant.* In the drop-down menu, select *Client fails one or more SHV checks,* which means that if a client fails to correctly report one or more required components from SHV, it will be considered unhealthy. Finally, select the Windows Security Health Validator check box and click OK.

Create Network Policies for NAP

After you configure the SHV and Health Policy options, you can configure network policies. In the NPS console's Policies node, click Network Policies and disable the default policies. By default, the two default policies are *Connections to Microsoft Routing and Remote Access Server* and *Connections to other access servers.* Right-click each policy and select Disable from the drop-down menu. Then, right-click the Network Policies folder and select New. A wizard for creating a new policy will start. Enter a policy name (e.g., "noncompliant-restricted" for a policy for unhealthy clients). Then, select from the drop-down list the type of network access server that will apply the policy to clients. The default is Unspecified; for our purposes, select DHCP Server.

Click Next to proceed to the Conditions page, and click Add to select conditions for the policy. From the list of available conditions that displays, select Health Policies from the Network Access Protection group. In the window that opens, select the "noncompliant" health policy that you created earlier.

Follow the same procedure to add the NAP-Capable condition, which Figure 4 shows, to the policy. This condition limits application of the policy only to computers that are NAP capable.

Click Next to launch the Specify Access Permission window. In this window, you must specify what to do with clients that meet the policy. Although denying access to unhealthy clients might seem logical, you don't want to completely deny access to those clients. Instead, you should provide them with limited access only to hosts that can help them improve their security state (i.e., remediation servers). Select Access Granted and click Next.

In the Configure Authentication Methods window, select the *Perform machine health check only* option, and clear the other check boxes, as Figure 5 shows. Because you're configuring a policy for checking clients' security health state via DHCP and because DHCP

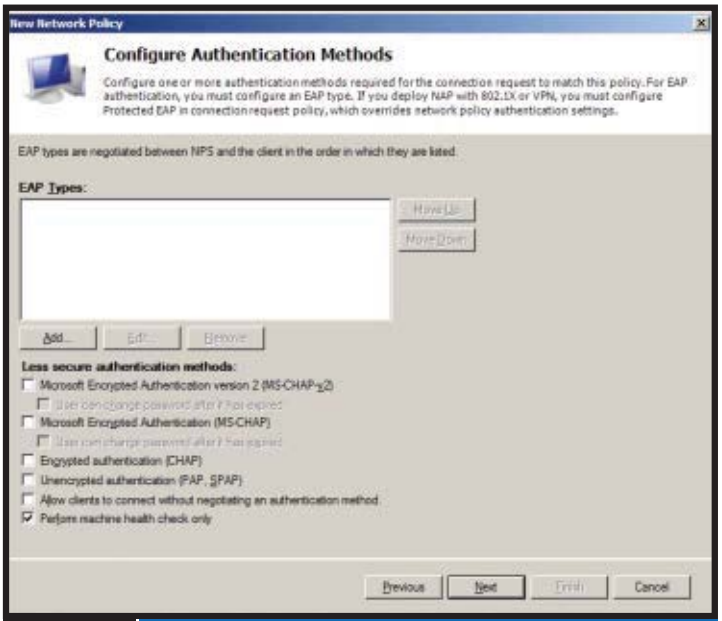


Figure 5: Configuring a policy for checking clients' security health state via DHCP

Protecting Your Data Records

Over 100 million private, proprietary data records have been lost or stolen in the last two years leading to loss of revenue and public embarrassment for many organizations. Understanding how to use technology during the collection, storage, backup, usage, retention, and destruction of proprietary data records can help mitigate information leakage. Use the resources in this learning path to help you simplify the task of protecting your data records.

Register today:
www.microsoft.com/technet/security/learning/dataprotection.mspx

Learning Paths for Security

Critical Security Information for IT Professionals

Learning Paths for Security is an online security curriculum where IT professionals can access the latest in security technology information, from the next big thing to how to solve today's security issues. Information is arranged by topic, technical depth (Level 100 through 400), and stage of the security lifecycle, so it's easy to find the information applicable to your specific situation and level of knowledge.

GUIDES
Download and print these white papers, resource kits, and articles to read and save for reference.

WEBCASTS
From Q&A sessions with experts on Microsoft® technology, the industry or both; to technical and product demos, these 60-90 minute broadcasts are available online so you can watch at any time, from any place.

ONLINE SEMINARS
These compilations of materials from a live event (including presentations, videos, and tools) are a quick way to get up-to-date on a topic of interest.

VIRTUAL AND HANDS-ON LABS
Test Microsoft software and servers in a sandbox environment.

TOOLS
Download free applications or software programs to help accomplish specific tasks you need to complete.

Learning Paths for Security can be found at:

www.microsoft.com/technet/security/learning

Microsoft

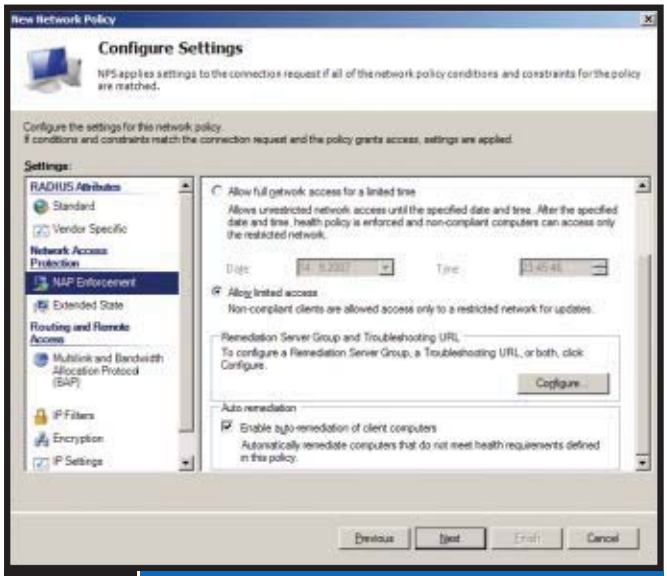


Figure 6: Configuring NAP enforcement

clients don't authenticate to the DHCP server, you don't need to configure authentication methods. Just click Next in the Configure Constraints window—none of the options apply to our example.

In the Configure Settings window, select NAP Enforcement in the Network Access Protection section, as Figure 6 shows. For this policy, you should select the *Allow limited access* NAP enforcement method. This setting will put clients in quarantine and give them access only to remediation servers. You can also configure those servers from this window: Simply click Configure to create a Remediation Server Group, and enter IP addresses for the hosts. Also select the *Enable auto-remediation of client computers* check box. Enabling both these settings causes the NAP Enforcement client component to automatically attempt to update the computer security state (e.g., if you turn the firewall off, it will be turned on automatically).

After you create a policy for incompliant clients, you must create a policy for compliant clients. Follow the same steps to create another new network policy, this time naming the policy "compliant full." On the Conditions page, select the "compliant" health policy. Then, select the *Allow full network access* check box on the NAP Enforcement Settings tab. All other settings are the same as for the incompliant client policy.

Finally, you can configure a policy for NAP non-capable clients, to provide them with or deny them network access. This policy should grant or deny access to clients that aren't NAP capable, by implementing only the NAP-Capable condition, with the *Only computers that are not NAP-capable* option selected. (Note that this policy isn't necessary in a test environment.)

Figure 7 shows the NPS console after you've created the necessary policies. Next, you need to configure DHCP.

Configure DHCP for NAP

You need to configure DHCP, so that DHCP can use NPS and the policies you created. First, you must create a scope on the DHCP server. Our intention is to configure the DHCP server to distribute a different group of scope options to compliant and incompliant NAP clients. After you create a scope, right-click it in the DHCP console. Select Properties, and go to the Network Access Protection tab. Then, select the *Enable for this scope* check box, as Figure 8 shows, and use the default NAP profile.

Another thing you can configure from the Network Access Protection tab in IPv4's properties is DHCP behavior, in case DHCP can't contact the network policy server. The default setting is to give clients full access, but you can also select the Restricted Access or Drop Client Packet options. In addition, you can enable and disable NAP on the server level.

Finally, you must configure additional options for NAP-capable clients. Right-click Scope Options, and select Configure Options.

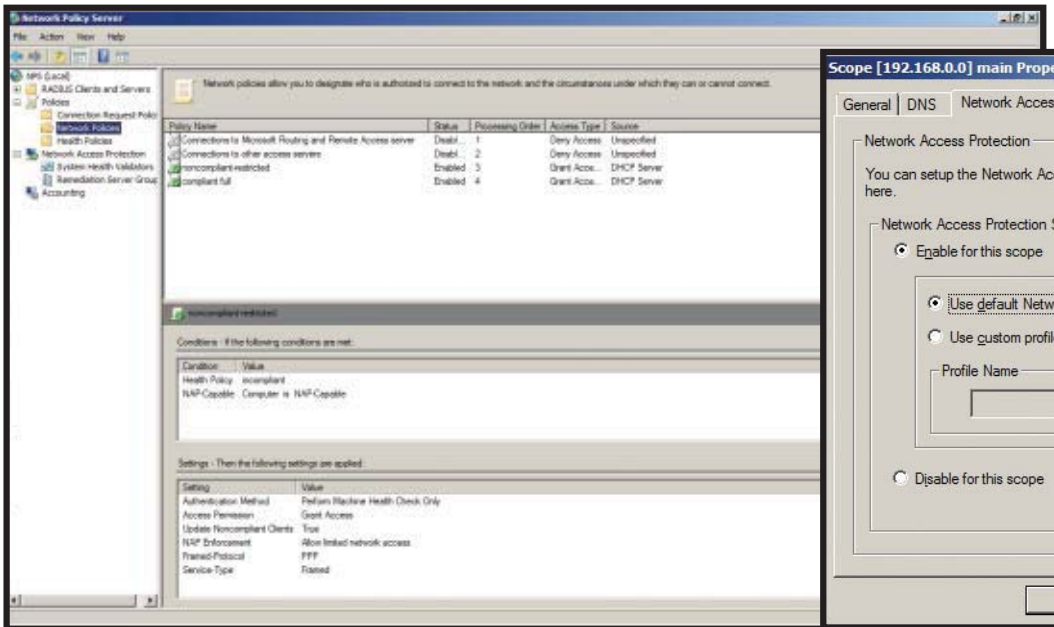


Figure 7: Viewing the NPS console after network policy creation

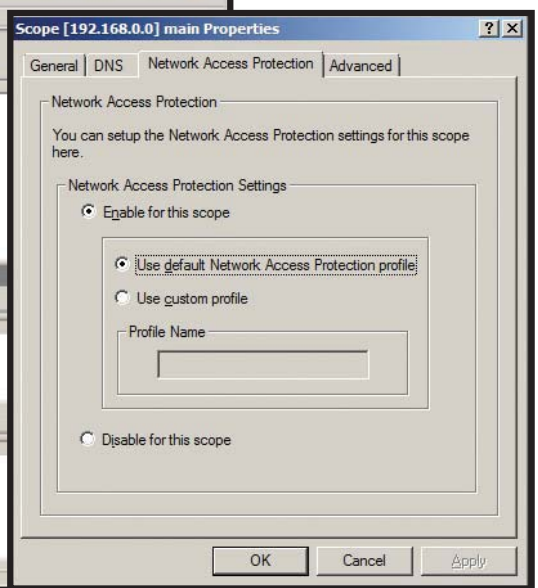


Figure 8: Enabling NAP on a DHCP scope

In the Configure Scope Options dialog box, select the Advanced tab. Select Default Network Access Protection Class as a User class, and define specific DHCP options for this class of clients (e.g., different DNS domain name, different gateway).

Enforce NAP on the Client Side

The last step is to configure the client to work with NAP. In fact, you must enforce the use of NAP on clients. You can accomplish this task through the NAP Client console, Group Policy, or Netsh (which has the new context for NAP configuration). Because you can't configure domain or OU Group Policy Objects (GPOs) to include NAP settings from Windows 2003, using Group Policy requires you to edit GPOs from Vista or Server 2008's Group Policy Management Console (GPMC). Use the Administrative Tools' Services console to start the Network Access Protection Agent service, changing this service's startup type to *Automatic* (which you can also use Group Policy to accomplish).

On Vista, start the Microsoft Management Console (MMC) and add the NAP Client Configuration snap-in. Alternatively, select Run from the Start menu, and enter

```
napclcfg.msc
```

Select the Enforcement Clients node in the left task pane, double-click *DHCP Quarantine Enforcement client* on the right side, select *Enable this enforcement client,* and click OK. From now on, the client should be able to use NAP.

To use Netsh to configure NAP on a client, go to the command line and enter

```
Netsh nap client set enforcement ID = 79617
```

If you want to use XP SP2, you must install the NAP client software for XP Beta 3, which makes the OS NAP capable.

Run a NAP Test

To test NAP on a client, configure a Vista client and join it to your domain. Obtain an IP address from the DHCP server, with the firewall in the default active state. Ensure that you have a regular IP address, from the scope that you created in earlier steps, with regular scope options. To verify that you have all the necessary DHCP information (e.g., DNS servers, gateway, WINS servers), go to the command line and enter

```
ipconfig /all
```

Figure 9 shows the output.

Next, manually disable the Vista firewall. In a few seconds, the DHCP enforcement client will perform autoremediation to correct the client's system state, thus reenabling the firewall. To demonstrate a quarantined client, go to Server 2008's NAP console and configure Windows Security Health Validator to require an antivirus application to be installed and updated. If you don't have an antivirus solution on the Vista client, run ipconfig /release followed by ipconfig /renew to quarantine your client and receive a taskbar quarantine notification message. Run ipconfig /all again, and note that your computer is configured with the options you specified in DHCP's Network Access Protection class. As Figure 10 shows, all you have is an IP address and subnet mask—no Internet access, and no access to other hosts on the network.

Figure 9: Results of testing NAP on a compliant machine

An Effective Solution

Maintaining computers' health is one of the most time-consuming challenges that any network administrator faces. This complex task is made even more difficult if you must maintain system health for users who connect from home systems, partner computers and laptops that aren't under control of administrators, or computers that aren't managed through a corporate patching system (e.g., Windows Server Update Services—WSUS, Microsoft Systems Management Server—SMS). NAP is an effective solution for controlling network computers' security health.

InstantDoc ID 95617

Damir Dizdarevic

(ddamir@logosoft.ba) is the manager of the Learning Center at Logosoft in Sarajevo, Bosnia. An MCSE, MCTS, MCITP, and MCT, he specializes in Windows Server security and has published more than 350 articles in IT magazines.

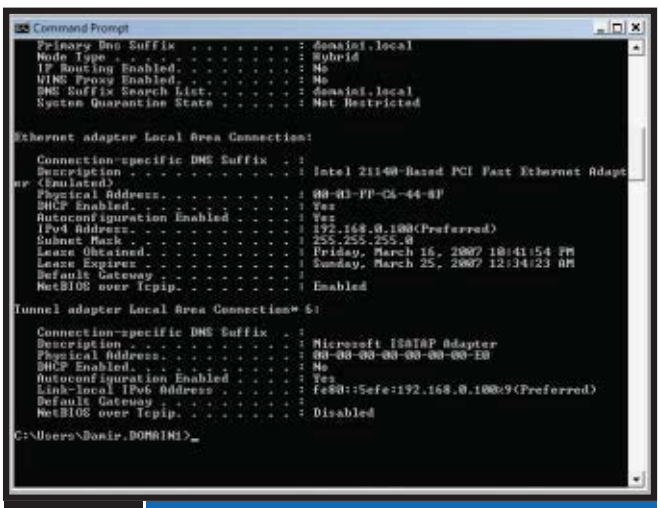


Figure 10: Results of testing NAP on an incompliant machine

… Tired of Nursing Your Exchange Server?

#1 BEST SELLER!

Anyone who has given birth to an Exchange network knows it can get sick and needs some nursing to stay healthy. In fact, 72% of Exchange Administrators surveyed* have "experienced" an Exchange disaster (feels like the flu)—usually from improper feeding and care.

Like many databases, constant adding and deleting can corrupt an Exchange data file so it eventually turns sour. Replicating, archiving and backing up the data doesn't stop the stink—it just stores it. You've got to…

Fix the Problem

You may have tried the free utilities to fix Exchange. While they help, they are too tedious, time consuming and lightweight to keep your Exchange baby healthy. You've tried the milk, now try some meat!

Pamper Yourself with GOexchange

It's time to try GOexchange, from Lucid8, the #1 best-selling automated disaster prevention and optimization software for Microsoft Exchange 5.5, 2000, 2003 and 2007. As the mother of all Exchange tools, GOexchange helps prevent disasters, repair problems, improves performance, and saves you a lot of time.

> *"Without routine maintenance, decreasing performance, increased warnings and errors accumulate and database fragmentation transpires, leading to Exchange disasters."*
>
> Gartner

Prevent Hiccups

GOexchange removes errors, warnings and inconsistencies within the database—before major corruption makes the database fail.

> *"GOexchange corrected 2,264 errors and 26 warnings."*
>
> Paul Ramos, Director IT

Run, Don't Crawl

In addition to fixing the database, GOexchange removes sluggishness and improves performance by re-indexing and defragmenting the database to permanently remove white space and deleted items. The end result is increased performance and stability with a compact efficient database that's 31 to 55% smaller! Combine this with archiving and the database is up to 91% smaller—making it much quicker to backup.

> *"..our information stores were reduced by 45-50%."*
>
> Dale Huitt, Systems Lead

Automated Babysitter

First, GOexchange is easy to setup and use. Twenty minutes—that's all it takes to get your server up and running. Just schedule it, and walk away!

The software notifies the users, validates the database, runs the backup, conducts a comprehensive system analysis and diagnostics, logs the errors, and notifies you if it discovers a "stop" error—then it repairs and defragments the database, generates a thorough report and schedules the next event.

You can do some of this work yourself, but why waste time doing repetitive maintenance, when GOexchange can do it for you—faster and more effectively than doing it by hand.

Created By

Lucid

Solutions Inspiring Confidence

> *"Life before GOexchange…was an absolute nightmare, late nights, long weekends and upset users."*
>
> Marty Grogan, CTO

Stop The Crying

Why not call now, or visit our resource site and learn how to reduce the risk, and avoid the pain. Protect your exchange data, maximize performance, and spend a weekend at home—*instead of babysitting Exchange.*

Special Offer

- **Free Software for analysis of your Exchange server!**
- **Free White Paper—"Basic Feeding of Your Exchange Server."**
- **Free Essential Guide to Exchange Preventative Maintenance**

Go to: www.Lucid8.com/GoITPro
Call 425.456.8474
E-mail: Sales@Lucid8.com

Securing Microsoft Exchange Server 2007

Start with a hardened Windows server and hosted filtering

Brien Posey
(www.brienposey.com) is the vice president of research for Relevant Technologies. He writes technical content for a variety of publications and Web sites.

Exchange Server 2007 is designed to be much more secure than its predecessors, but it would take a thick book to tell you all you need to know about Exchange 2007 security. After all, securing Exchange 2007 includes everything from creating a high-level architectural design to tweaking dozens of obscure settings deep within the product.

My personal philosophy has always been that security must be applied in layers. Tweaking a bunch of security settings won't do you much good if you have gaping security holes throughout your Exchange organization. That being the case, I'll focus this article on designing a secure Exchange Server organization, discussing fundamental, big-picture practices such as limiting yourself to one version of Exchange and using the different Exchange roles wisely. If you start with a secure design, you greatly increase the chances that the security settings you implement later on will be effective.

Harden Windows and Use Firewalls

The majority of the security steps that I talk about in this article have to do with the design of your Exchange organization rather than the deployment process. I want to quickly mention, though, that when it does come time to deploy Exchange, one of the most important things to do from a security standpoint is to harden Windows before you ever even install Exchange.

Exchange Server is completely dependent upon the Windows OS. If your Windows implementation has weak security, then your Exchange implementation will also have weak security. Therefore, it's extremely important that you remove all unnecessary Windows components and services, install all the latest Windows patches, and follow the various security best practices for Windows. You can get more specific information from the *Windows Server 2003 Security Guide,* which you can download at www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx You can also use the Security Configuration Wizard to help you to harden your servers and reduce their potential attack surface. You can download the Security Configuration Wizard at www.microsoft.com/downloads/details.aspx?familyid=903fd496-9eb9-4a45-aa00-3f2f20fd6171&displaylang=en.

Furthermore, it's extremely important that your organization use a solid firewall configuration. My personal recommendation is to take a layered approach to firewalls. Your network perimeter should be protected by a firewall appliance, but I also recommend placing a Microsoft ISA Server system just inside your perimeter network. ISA Server was developed with Exchange Server in mind and makes an effective application firewall. Even with ISA Server in place, though, you should use the Windows firewall on each of your servers as a way of preventing attacks that may occur from within your organization.

Use Only 1 Exchange Version

In my opinion, one important aspect of developing a secure Exchange Server organization is maintaining strict control over both Exchange and Windows server versions. For example, if you're getting ready to move to Exchange Server 2007, then I think it's better from a security (and, certainly, management) standpoint to deploy Exchange 2007 on all your Exchange servers than to have a mixture of Exchange 2007 and Exchange Server 2003.

A lot of you are probably having a fit after reading that last statement. After all, Microsoft fully supports coexistence between Exchange 2007, Exchange 2003, and Exchange 2000 Server. Hear me out, though.

One reason why I recommend trying to limit your organization to one Exchange version is that by doing so, you reduce management complexity. For example, Exchange 2003 requires the use of sites, routing groups, and administrative groups. These features were removed from Exchange 2007, but Exchange 2007 can emulate these features to remain backward-compatible with the earlier version. By removing Exchange 2003 from your organization, you eliminate Exchange Server 2007's need to emulate these features, thus reducing the complexity of the code that's running.

My general rule of thumb when designing an Exchange Server organization is that you should reduce complexity anywhere possible. Doing so often improves security and makes troubleshooting any problems easier.

Another reason why I believe that staying with one Exchange version is important is that it helps eliminate the "what if" factor. Imagine, for example, that you're running Exchange 2007 and Exchange 2003. Now suppose that someone discovers a huge security flaw related to the way Exchange 2007 interacts with the server's transport stack. (This isn't a real problem, it's just an example.)

In a situation like this, it's appropriate to wonder whether the vulnerability is unique to Exchange 2007 or also exists in Exchange 2003. If all your Exchange servers were running Exchange 2007, you simply focus your attention on patching the known bug, rather than trying to determine whether another version of Exchange has a similar bug.

Put Only 1 Exchange Server Role on Each Server

The concept of server roles isn't new to Exchange 2007, but this version takes the role concept much further than Exchange 2003 does. The only roles that formally exist in Exchange 2003 are those of front-end and back-end Microsoft Outlook Web Access (OWA) servers. Many administrators "define" their own Exchange 2003 roles, such as mailbox servers and public folder servers. In fact, Microsoft introduced other roles in the *Microsoft Exchange Server 2003 Security Hardening Guide* (www.microsoft.com/downloads/details.aspx?familyid=6A80711F-E5C9-4AEF-9A44-504DB09B9065&displaylang=en) but didn't implement them in Exchange 2003 itself.

Exchange 2007 has five server roles and requires you to select the ones that you want to use during the initial Exchange installation. Of course, you also have the option of adding and removing server roles as your needs change.

The five roles are Mailbox, Client Access, Hub Transport, Edge Transport, and Unified Messaging. A single server can host multiple roles. The only roles that can't work with other roles are the Edge Transport role, and the Mailbox role if the server is clustered. I discuss the Edge Transport server role in more detail later. Right now, though, I want to focus attention on the other four roles and how to design a secure Exchange environment with these roles in mind.

Learning Path

To publish Exchange 2007 on ISA Server 2006:

"Securing Exchange Server 2007 Services with ISA Server 2006," Security Pro VIP, InstantDoc ID 96957

"Publishing Exchange Server 2007 with ISA Server 2006" www.microsoft.com/technet/isa/2006/deployment/exchange.mspx

For more guidance on Exchange 2007 server roles:

"Exchange 2007 Server Roles and You," *Exchange & Outlook UPDATE*, InstantDoc ID 53882

"Fight Spam Using Exchange 2007's Edge Server Role," Security Pro VIP, InstantDoc ID 95961

For more information about hosted filtering:

"Antispam Solutions for Business," InstantDoc ID 94326

"FrontBridge Gets a Makeover," *Exchange & Outlook UPDATE*, InstantDoc ID 49910

The Edge Transport role aside, a single Exchange server can run any combination of the various server roles. In fact, if you aren't using the Edge Transport role, it's possible to have one Exchange 2007 box that runs all the Exchange server roles simultaneously. However, for both security and performance reasons, I recommend that each Exchange server host only one role.

Servers running the Mailbox role host Exchange mailbox and/or public folder databases. It's common practice to dedicate one or more servers to running the Mailbox server role, but the reason is typically related more to performance than security. Exchange databases tend to be resource hogs, so a dedicated server makes sense in many situations.

If you must consolidate server roles, then I recommend running the Mailbox role and the Hub Transport role on the same box (assuming that your hardware is up to the job). These two roles present the least chance of causing a security problem when run together.

Hub Transport servers are responsible for all internal mail flow, routing messages and applying filtering rules to them. Because this role and the Mailbox role both sit on the internal network, the security risks associated with running these two roles on the same box are minimal.

The Client Access role should always run on a dedicated server. This role is the Exchange 2007 equivalent of an Exchange 2003 front-end OWA server, meaning that it receives requests from the Internet and forwards them to a Mailbox server. Obviously, you should have a firewall sitting in front of the Client Access server filtering out everything except HTTP and HTTP Secure (HTTPS) traffic on ports 80 and 443. Even so, the Client Access role does receive traffic from the Internet, and it's best to not have the Client Access server hosting other roles that could potentially be exploited.

The Unified Messaging role is completely new to Exchange 2007. In case you're not familiar with unified messaging, it's a new technology that allows voice messages and faxes to be received and stored alongside email messages. Unified Messaging servers provide a new type of interface called Outlook Voice Access (OVA), which lets users interact with the Exchange organization by using their voice or touch tones via a telephone.

In my opinion, OVA doesn't pose nearly the security risks that OWA does because OVA doesn't expose Unified Messaging servers to the Internet, and Unified Messaging users don't use a computer to connect to the servers. However, OVA does expose Unified Messaging servers to the Public Switched Telephone Network (PSTN), which arguably has worse security and more connected devices than the Internet. Thus, I recommend isolating Unified Messaging servers from the rest of the Exchange server organization with a firewall. In addition, Unified Messaging servers are extremely resource intensive and that condition alone often justifies using a dedicated server.

Employ an Edge Transport Server

The Edge Transport server role is new in Exchange 2007. I want to talk about this role separately because its entire purpose is to help secure the Exchange organization. I recommend that every Exchange environment uses an Edge Transport server as an important part of its security plan.

Using an Edge Transport server role is like bringing hosted filtering in house. If you aren't familiar with hosted filtering, I discuss it next. An Edge Transport server sits behind the corporate firewall but is isolated from the rest of your Exchange server organization, usually on a separate network segment. The Edge Transport server filters messages before they enter your primary Exchange organization to get rid of viruses and spam, thus helping to lighten the workload of your Mailbox servers and Hub Transport server.

Having an Exchange server that's dedicated to the task of removing viruses and spam before messages pass through to your internal network probably sounds like a good idea, but you might be apprehensive to deploy an Exchange server, with its dependency on Active Directory (AD), on the edge of your network. Earlier I mentioned that the Edge Transport role can't coexist on a system with any other Exchange role. This is because Microsoft designed Exchange 2007 so that servers running the Edge Transport role don't need AD access (at least not directly).

To avoid exposing AD to the outside world, an Edge Transport server relies on AD Application Mode (ADAM) instead. ADAM is an AD partition that stores data related to a specific application rather than storing a copy of the entire AD database. When you install the Edge Transport role, Exchange creates an ADAM database on the Edge Transport server.

STEPS TO PROTECT Your Exchange 2007 Organization

Step 1 Harden Windows and use firewalls.

Step 2 Limit yourself to one Exchange version.

Step 3 Put only one Exchange server role on each server.

Step 4 Employ an Edge Transport server.

Step 5 Choose hosted filtering.

InstantDoc ID 97081

A minimal amount of information is then pushed from AD to the ADAM database to give the Edge Transport server the configuration information it needs, without exposing all of AD in the process.

Microsoft even designed the Edge Transport replication process to prevent exposure. The Edge Transport server never contacts the rest of the Exchange organization. Instead, the setup process creates a special XML file, called an edge subscription file, on the Edge Transport server. The edge subscription file tells your Exchange organization to replicate recipient and configuration information from AD to the ADAM partition on the Edge Transport server. The administrator copies this file to the Hub Transport server and then manually removes it from the Edge Transport server so that a hacker can't use this file to exploit the replication process.

Given its role within the organization, an Edge Transport server is designed to be secure by default. As such, there isn't anything special that you have to do to secure an Edge Transport server aside from making sure that Windows is installed securely, removing the edge subscription file, and following routine best practices that are common to all Exchange servers.

Choose Hosted Filtering

I'm a big believer in hosted filtering, in which a company such as an ISP filters out viruses and spam before they ever reach your Exchange organization. When hosted filtering is in use, the MX record for your domain doesn't point to your mail server but rather to a designated IP address that belongs on the server that's filtering content. This means that email doesn't come directly to your organization but flows to the filtering company first. The filtering company scans for and removes viruses and spam and then forwards legitimate messages to your Exchange organization.

Hosted filtering offers at least three benefits. First, email viruses are eradicated by the filtering server and never reach your organization. I still recommend running antivirus software on your Exchange servers and email client machines, though. You never know when a virus might slip through the hosting company's filter, and having your own antivirus software is a good second line of defense.

The second advantage of hosted filtering is that it helps to conserve network bandwidth. It's probably safe to say that in most organizations, spam accounts for 60 percent to 90 percent of the total inbound email. If you can filter out most spam before it reaches your organization, you could end up saving a significant amount of Internet bandwidth just because your Exchange servers don't have to download all that spam. Not only does blocking spam reduce Internet bandwidth consumption, but it also helps to conserve memory, CPU, and disk resources on your mail servers.

The third major benefit of hosted filtering is that it obscures your mail server's IP address from the outside world. The DNS record that would normally point to your mail server now points to a filtering server that's part of another company's network. A hacker who attacks your mail server might not realize that you use hosted filtering and might directly attack the filtering company rather than you. A more sophisticated hacker might be able to determine your mail server's real IP address, but locating it would be more difficult than it would be if hosted filtering weren't in use.

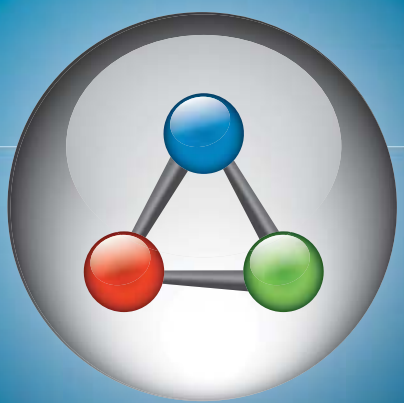
This article just barely scratches the surface of what you need to know about Exchange security. Even so, good security starts with a secure design, and I've talked about some things that you can do to design your Exchange organization with security in mind.

InstantDoc ID 97079

busi·ness
pro·cess
au·to·ma·tion

[biz-nis | pros-es | aw-tuh-mey-shuhn]

The replacement of a manual business process with an automated one, usually through the use of **advanced technologies**.



AutoMate BPA Server 7™

The Business Process Automation Server from Network Automation

NO CODE, NO LIMITS

Automates business & IT processes
Eliminates the need for job schedulers, scripts & batch files
Intuitive drag-and-drop workflow design & task development

Visit **WhatIsBPAServer.com** to learn more about **BPA Server 7** and how the world leader in **Business Process Automation** is advancing the field. Again.

NETWORK AUTOMATION

www.WhatIsBPAServer.com
888-786-4796

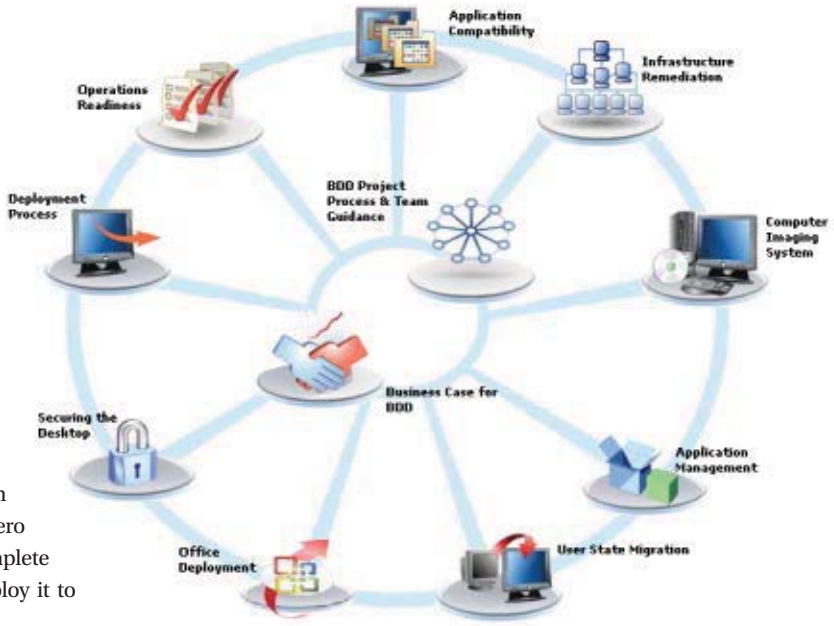
Redmond MVP Most Valuable Product

Windows IT Pro READERS CHOICE 2006 Winner

Windows IT Pro EDITOR'S BEST 2007 WINNER

Using Deployment Workbench

Rhonda Layfield
(rhonda@minasi.com) is a consultant and trainer.



In the Learning Path article "Planning Your Vista Deployment with BDD" (October 2007, InstantDoc ID 96906), I began a tour through the Microsoft Solution Accelerator for Business Desktop Deployment 2007 (BDD) tool by explaining how to install and run the BDD tools that make planning for a Windows Vista upgrade and deployment a lot easier. In this article, I continue the journey by exploring Deployment Workbench, a BDD toolset that helps you automate your Windows Vista and other OS deployments and manage multiple OS configurations. I'll step you through the basics of a Lite Touch Installation (LTI—my next article in this series about BDD will focus on Zero Touch installs). We'll create a generic Vista installation complete with applications, patches, and out-of-box drivers and deploy it to target machines.

Getting Started

If you haven't already done so, download and install BDD 2007 as "Planning Your Vista Deployment with BDD" describes. Next, log on as an administrator and open Deployment Workbench from Start/All Programs/ BDD 2007/ Deployment Workbench.

Deployment Workbench is a Microsoft Management Console (MMC) 3.0 snap-in whose default view includes an Actions pane that displays the same menu options that you'd see by right-clicking an object. I recommend closing the Actions pane so that you have more room on the desktop. Most of Microsoft's MMC 3.0 snap-ins have a button that lets you hide or show the Actions pane, but Deployment Workbench does not. To remove the Actions pane for good (not just from the single instance of Deployment Workbench you've launched), you must edit the Deployment/Workbench.msc file. To do so, click Start, Run; browse to C:\Program Files\BDD 2007\Bin\DeploymentWorkbench.msc; append the /a switch to the end of the run statement; then execute the command. Deployment Workbench will open in editable mode (aka author mode). From the View menu, click Customize, clear the *Actions pane* check box, then click OK. Close MMC by clicking the white X in the top right-hand corner. You'll be prompted to save the console settings: Choose Yes to save the display in a single window interface.

When you installed BDD, a folder named Distribution was created on a drive on your machine that has the most available free space. The Distribution folder contains subfolders that correspond to Deployment Workbench's subnodes. As you add components to Deployment Workbench, XML files are created to contain metadata about the components. To easily browse and edit these XML files, I recommend that you download and install a free Microsoft tool called XML Notepad (available from www.microsoft.com/downloads/details.aspx?FamilyID=72D6AA49-787D-4118-BA5F-4F30FE913628&displaylang=en).

Easily create and deploy a new Vista installation with this BDD tool

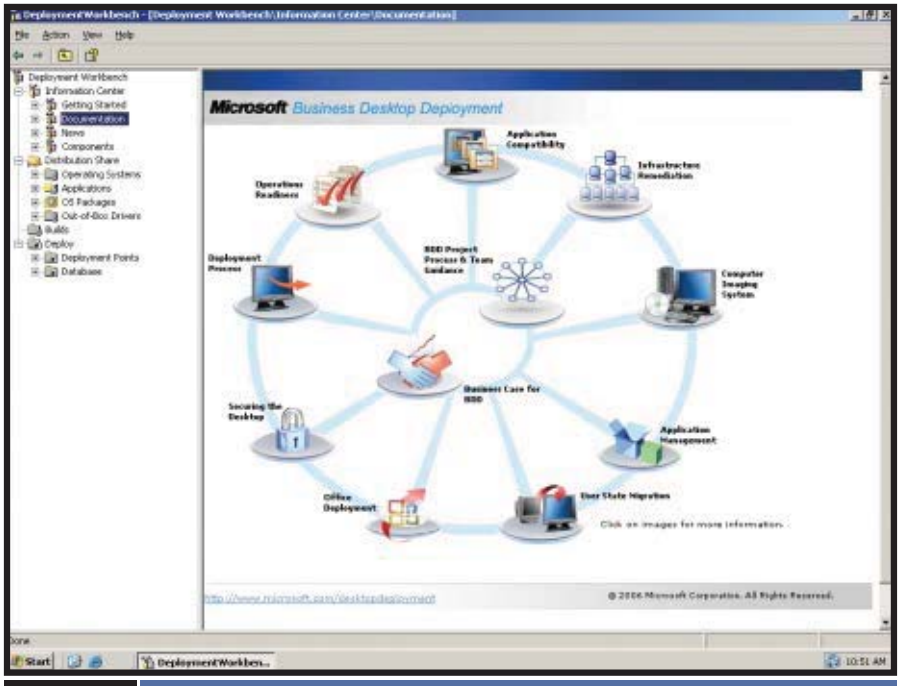


Figure 1: The Deployment Workbench console

Inside Deployment Workbench

Deployment Workbench has four nodes, which Figure 1 shows: Information Center, Distribution Share, Builds, and Deploy. The Information Center node thoroughly documents Deployment Workbench; Microsoft has outdone itself with this documentation set. Distribution Share introduces OS images and patches, applications, and third-party out-of-the-box drivers to Deployment Workbench. The Builds node groups OS images and drivers as well as some settings for the installation, and the Deploy node contains your *deployment points,* the locations to which target machines connect to install the new Vista *build* you will create and distribute.

Beware of a quirk in Deployment Workbench: If you open more than one instance at a time, Deployment Workbench exhibits unpredictable—and annoying—behavior. (Every time I opened two instances of Deployment Workbench, both instances would freeze.) Avoid problems by having only one instance open at a time.

Adding an OS

Let's begin our new Vista deployment by launching the New OS Wizard: Expand the Distribution Share node in the Deployment Workbench console tree, right-click Operating Systems, and choose New. For the first OS you add, you must choose *Full set of source files* from the wizard's *Choose the type of operating system to add* page, which Figure 2 shows. The *Full set of source files* option copies all files, including setup.exe.

It appears as though you have a choice as to the type of OS to add, but you really don't. If you select either *Custom image file* or *Windows Deployment Services images* before you add a full set of source files, you'll be met with a "Lite Touch Installation is failed" with the error code (0x00000001) when you attempt to deploy the installation image to a target machine. After you've added a full set of OS files, you can add additional OSs from custom OSs from custom Windows Imaging Format (WIM) files or from images stored on a Windows Deployment Services (WDS) server. The *Custom image file* option requires you to enter the path of the .wim file you want to use. The *Windows Deployment Services images* option lets you point to a WDS server that contains images you've previously created. (For more information about WDS, see this article's Learning Path.) If a .wim file doesn't contain a necessary OS file, the .wim file will use the file from the "Full set of source files" that you originally added.

After you choose *Full set of source files* and click Next, you'll be prompted for the path to the Vista OS files. The wizard's final page asks for the name of the folder in which to create and store the OS.

Adding Applications

Now that you've introduced the Vista image, it's time to add the applications that you want to deploy with the OS. Begin by launching the New Application Wizard in Distribution Share: Right-click Applications, then click New. Select either *Application with source files* or *Application without source files or is elsewhere on the network.* If you choose the second option, you can specify a Universal Naming Convention (UNC) path (i.e., *servername**sharename*) to the application's location. You can use Distributed File System Namespace (DFSN) and Distributed File System Replication (DFSR) to group and replicate multiple applications.

You'll need to supply the wizard with the application's name, source directory, and supported platform (your choices are *All platforms*, x*86 only*, *x64 (amd64) only*, and *ia64 only*); the name of the directory for the wizard to create in the Distribution\Applications folder; the command line to be run in quiet mode; and the working directory to begin the command from. Figure 3, page 62, shows how applications are listed in the Applications subnode.

An Applications.xml file is created in the Distribution\Control folder and contains information on all applications you add to Deployment Workbench. Each application is given its own globally unique identifier (GUID) in the Applications.xml file. To edit an applica-

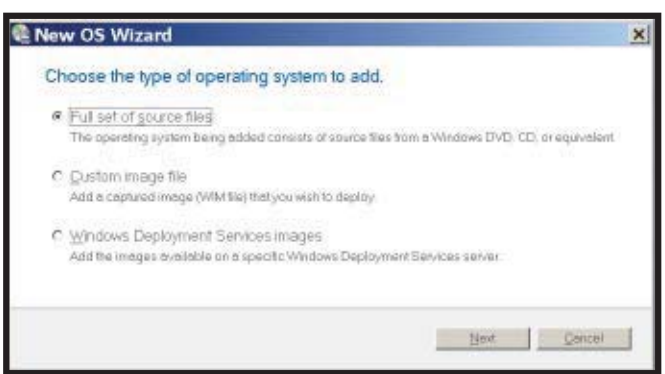


Figure 2: Adding a full set of source files

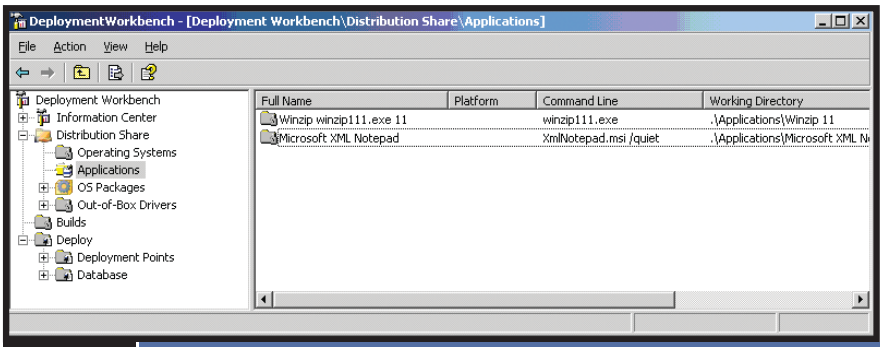


Figure 3: A list of added applications

tion, double-click the application name to view its properties. There are two tabs on an application's properties page: Dependencies and General. The Dependencies tab lets you specify applications that must be installed prior to this application being installed. If the dependent applications aren't installed, the application you've added will fail to install.

Adding Vista Security Updates, Service Packs, and Language Packs

Next, launch the New Package Wizard from Distribution Share to add Vista security updates, service packs, and language packs to your Vista image: Right-click OS Packages, then click New. You'll be prompted for the paths to the folders that contains these patches; the wizard will add everything a folder contains to Deployment Workbench.

Adding Drivers

Launch the New Driver Wizard from Distribution Share by right-clicking Out-of-Box Drivers, then click New. The wizard prompts for the folders that contains the drivers you want to add to Deployment Workbench and adds everything a folder contains.

Creating a Build

Up to this point, you've introduced to Deployment Workbench all the components you want to install on target machines. Now let's add those components to the build that Deployment Workbench will deploy. To begin, launch the New Build Wizard under Distribution Share by right-clicking Builds, then clicking New. The wizard will ask you to create a Build ID, such as "Vista01" (the ID can't contain spaces) and a descriptive *Build name*, such as "Vista Build for VPs." A field exists where you can add comments, and there's plenty of room to document what's in your build and why. The New Build Wizard lets you choose an OS to associate to this build (the list of OSs is based on what you added earlier in the Distribution/Operating Systems node). You can specify a product key for the OS at this time or not (you might want someone to enter a product key for each install). Next, specify the name, organization, and Microsoft Internet Explorer (IE) home page that will be used for all installations from this build. Finally, type in the local administrator's password or specify that you don't want to use a password, and click Create.

You can access your build's properties by double-clicking the build name under Builds. The build properties page has three tabs. On the General tab, you can edit any unshaded properties and enable or disable the build. The Settings tab lets you edit *Organization name*, *Full name*, *Local administrator password*, *Internet Explorer home page*, and product key information.

If you're familiar with Microsoft System Center Configuration Manager (SCCM), then you've already met the task sequencer, which lets you add tasks to your installation in the exact order they should occur. Maybe you want to add a task (perhaps as another way to add patches) after the installation is complete. Highlight the Postinstall node on the Task Sequence tab, click the Add button, and choose Task. Give your new task a name and description and specify the command line to run and the location to run it from. On the Options tab of your new task you can choose *Disable this step* (I like this for troubleshooting purposes), *continue on error*, or *create dependencies for the successful completion of this task*.

Creating a Deployment Point

Next, use the New Deployment Point Wizard to create the deployment point, the location to which target machines connect to install a build. To launch the wizard, expand the Deploy node in the console tree, right-click Deployment Points, and click New. The wizard will prompt you to choose from among four deployment point types: *Lab or single server deployment*, the default option, uses the deployment share on the computer on which Deployment Workbench is running; *Separate deployment share* lets you provide a UNC path to a server and share of your choice; *Removable media* lets you create a shared folder to use to create images for deployment on removable media; *SMS 2003 Operating System Deployment (OSD) Feature Pack*, lets you create a

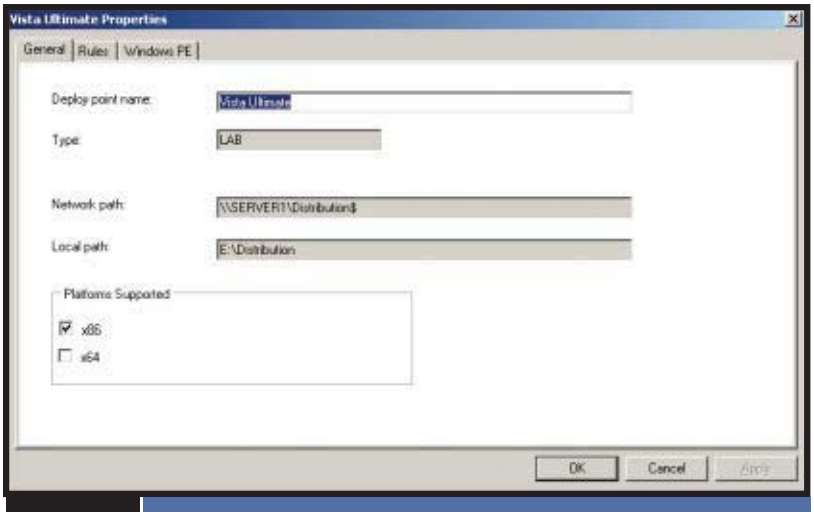


Figure 4: A deployment point's properties page General tab

Microsoft

Assess, deploy and update from the desktop to the datacenter and beyond.

Automate Your Windows® Deployments with Microsoft® System Center Configuration Manager 2007

Are you looking for a desktop and server deployment solution designed to scale? System Center Configuration Manager 2007 together with the Microsoft Deployment Solution Accelerator provide the tools and methodology to fully automate and manage large-scale deployments of server and desktop operating systems.

The data and automation you need for the job — upgrade assessment, hardware and software inventories, disk imaging, data migration, application compatibility testing and zero touch operating system installation — can be managed with a streamlined task sequencer in System Center Configuration Manager 2007, while a driver catalog works to reduce the number of images. System Center Configuration Manager 2007 is built on and optimized for Windows.

Go to www.microsoft.com/systemcenter/configmgr and discover the new path to consistent, scalable and successful deployments.

Windows Vista

Windows Server 2008

Microsoft® System Center Configuration Manager 2007

shared folder for creating Microsoft Systems Management Server (SMS) OSD Feature Pack images (I'll cover this option in more detail in my next article in this series).

Subsequent wizard pages prompt you to give your deployment point a name, choose whether to allow users to select additional applications to be installed during an upgrade, and specify whether to prompt users to capture an image of the target computer (for our sample deployment, clear the *Ask If an Image Should Be Captured* check box). Next, specify whether to prompt users to provide the local administrator password for target computers and whether to prompt users to provide a product key. Finally, specify the server and share name of the deployment point, specify whether users will be prompted to save user state migration options, and click Create. Nothing substantial happens just yet, but a deploy.xml file is created in the Distribution\Control folder.

What really gets things rolling is updating your deployment point. To do so, right-click the deployment point name under Deploy/Deployment Points, and choose Update. A Microsoft Windows Preinstallation Environment (WinPE) file, LiteTouchPE_x86, is created in the Distribution\Boot folder and is converted to a bootable ISO file, LiteTouchPE_x86.iso. Three files are created in the Distribution\Control folder: Bootstrap.ini contains the UNC path to the deployment point; CustomSettings.ini contains your selections in the New Deployment Point Wizard; TS.xml contains the task sequencer list of tasks and the order in which they are to be performed when a target machine connects to the deployment point.

To see the deployment point's properties, double-click the deployment point's name in the console tree. The properties page has three tabs. The General tab, which Figure 4, page 62, shows, displays the deployment point's name and type, the UNC and local path to the shared folder, and the platforms that the deployment point supports.

The Rules tab contains the settings from the CustomSettings.ini file that determine which screens will display during the installation. You can edit the UNC path to your deployment point by clicking *Edit Bootstrap.ini* on the Rules tab and entering your changes.

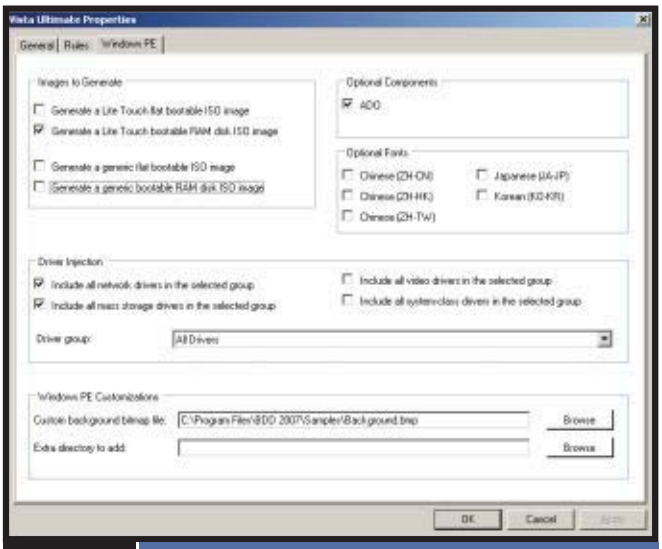


Figure 5: A deployment point's properties page Windows PE tab

The Windows PE tab, which Figure 5 shows, gives you options for controlling how your WinPE file is configured. You can generate a Lite Touch bootable ISO image that contains scripts for connecting to the deployment server, or you can create a generic ISO image. You can also choose additional language support (i.e., optional fonts), specify driver groups to be installed, add a custom background bitmap file for the desktop, and add directories to the WinPE file.

Deployment

Now it's time to boot the target machines and begin the deployment. Target machines must boot from the WinPE file that the New Deployment Point Wizard created. You'll have two WinPE files by default: LiteTouchPE_x86.iso and LiteTouchPE_x86.wim. To boot from LiteTouchPE_x86.iso, you must first burn it to a CD-ROM or DVD. To boot from LiteTouchPE_x86.wim, add it to your WDS server. Storing this .wim file on your WDS server lets you PXE boot (F12 for a network boot) your target computers, connect to the WDS server, and boot the custom WinPE file.

Whichever method you use to boot the target machines, your custom WinPE file contains scripts that direct the target machines to connect to the deployment point and read the rules for the installation. With the default set of rules, the target machines will launch the Welcome Windows Deployment screen. On this screen, choose your desired Keyboard Layout from the drop-down menu, and click Next to start the Windows Deployment Wizard. You'll be prompted for credentials to the deployment point: The account you use must have read, write, and execute permissions to the deployment point. Click Next. The next pages ask you to supply the target computer's name, credentials for joining the target computer to a domain or workgroup, whether you want to restore users data (e.g., if you had previously saved users' IE favorites, My Documents, and other settings with User State Migration Tool—USMT). Next, you'll choose a build, choose whether to provide a product key, and specify language settings and time zone. A list of applications that you've added to the deployment point will appear, and you can specify from the list which applications you want to deploy. Finally, supply the local administrator password and specify whether BitLocker is to be enabled on the target machine, and if so, where the BitLocker key is to be stored, then click Create. A progress box will display, and if you watch it closely, you'll see all the steps that the deployment process goes through. When the progress bar reports a successful completion, you'll have brand-new Vista machines with all your applications, patches, and out-of-box drivers installed perfectly—again and again and again.

InstantDoc ID 97170

Learning Path

WINDOWS IT PRO RESOURCES

Let WDS Ease Your Vista Rollout Pain, InstantDoc ID 96098

What's the Windows Preinstallation Environment (WinPE)? InstantDoc ID 38308

MICROSOFT RESOURCES

"BDD 2007 Demo"
www.microsoft.com/technet/desktopdeployment/demos/index.html

"Lite Touch Installation Guide"
technet.microsoft.com/en-us/library/bb456433.aspx

"Microsoft Solution Accelerator for Business Desktop Deployment 2007"
technet.microsoft.com/en-us/library/bb490308.aspx

Office & SharePoint PRO

officeandsharepointpro.com

Automating Office 2007 Deployment

Economical and practical methods for deploying the latest version of Office

by Dan Holme

A few months ago, in "Customizing and Deploying Office 2007," May 2007, InstantDoc 95433, I walked through how to deploy Microsoft Office 2007 by creating a network installation point with a series of customizations, including setup customization (.msp) files and configuration (config.xml) files, to drive the behavior of Office Setup. Now that you've had time to prepare an installation of Office 2007, you can turn to the task of deploying Office 2007 to your clients. Let's take a quick look at some familiar deployment methods that, unfortunately, aren't necessarily ideal for Office 2007, then explore workarounds for deploying Office 2007 that won't stretch your budget. You can also use these workaround methods to deploy other software and configurations—sort of a do-it-yourself Systems Center Configuration Manager.

Preferred Deployment Methods and Dead Ends

For software deployment, several methods come to mind. The first method is to use Group Policy Software Installation (GPSI) to deploy Office .msi files. Three previous Office versions could be deployed using GPSI, however, deploying Office 2007 using GPSI isn't really a feasible option. Nevertheless, Microsoft documents how to deploy Office 2007 using GPSI (see "Use Group Policy Software Installation to deploy the 2007 Office system" at technet2.microsoft.com/Office/en-us/library/efd0ee45-9605-42d3-9798-3b698fff3e081033.mspx), and Darren Mar-Elia discusses the Group Policy deployment of Office 2007 in "The Group Policy Route to Office Deployment and Management," April 2007, InstantDoc ID 95210.

Despite what these information sources say, I can tell you from my experience doing lots of testing that deploying Office 2007 using GPSI isn't practical, even if it's technically doable. GPSI uses .msi files with transforms (.mst files), whereas Microsoft architected Office Setup to use the Setup command (setup.exe) with .msp files to drive installation, so you'll find that GPSI doesn't support the kind of functionality and customization that you need. With GPSI, you must perform all customizations in the config.xml file, and even then you can customize only a few settings, such as the product key, language, and applications to install. And trying to configure which applications to install by using the OptionState element of the config.xml file is painful to say the least. The aforementioned Microsoft article provides information about how to use OptionState if you're so inclined to self-torture. You can try deploying Office 2007 by using GPSI, but I expect you'll find, like most organizations, that it's just not full-featured enough to be useful.

A second deployment option is to use GPSI to deploy Office 2007 by using a .zap file. A .zap file is a simple script that can call any command—in this case, it would call Office's setup.exe command with all its switches. GPSI can deploy a software package with a .zap file; you just have to select the .zap file instead of an .msi file when creating the package. However, .zap files can only be published, not installed, so that Office can appear in the Add/Remove Programs list under Programs and Features in Windows Vista and can even be

Learning Path

WINDOWS IT PRO RESOURCES

For more information about deploying Office 2007

"Customizing and Deploying Office 2007," InstantDoc ID 95433

"The Group Policy Route to Office Deployment and Management," InstantDoc ID 95210

MICROSOFT RESOURCES

"Use Group Policy Software Installation to deploy the 2007 Office system"
technet2.microsoft.com/Office/en-us/library/efd0ee45-9605-42d3-9798-3b698fff3e081033.mspx

Listing 1: Office2007_Deploy.vbs

```
Option Explicit

' BEGIN CONFIGURATION BLOCK

' DOMAIN
Dim sDomainDNS, sDomainDN
sDomainDNS = "windomain.com"
sDomainDN = "dc=windomain,dc=com"

' DATABASE DEFINITION: where our script will find its data store
' The database is used to log the results of the script
' Because systems don't yet have Office 2007,
' use a downlevel database format (xls/mdb)
Dim sFile, sTable
sFile = "\\server01.windomain.com\configmgt\SystemConfigurationDB.xls"
sTable = "Sheet1" ' Name of Excel sheet or Access table
Dim sComputerNameField, sActionField, sStatusField, sDateField, sNotesField
' Data table (e.g. Excel worksheet) consists of fields/columns
' labeled as defined below.
' The items on the right side of the equal sign
' should be the labels in the first row of the worksheet
sComputerNameField = "ComputerName"
sActionField = "Action"
sStatusField = "Status"
sDateField = "Date"
sNotesField = "Notes"

Dim sCommand
' COMMAND to run Office 2007 installation
sCommand = "\\windomain.com\software\office\setup.exe"

Dim sAction
' ACTION that will be logged in the ACTION column of the log
sAction = "Office 2007 Deployment"

Dim sStagingGroup, sSuccessGroup, sErrorGroup
' GROUPS that manage this change
' Important: These groups must have the access control entry
'     SELF::Allow::Write::Members
' Group that computer/user is in BEFORE this script is run
sStagingGroup = "CCM_Office 2007 Deploy"
' Group that this computer/user is moved to based on success
sSuccessGroup = "APP_Office 2007"
sErrorGroup = "ALERT_Office 2007 Deploy"

' END CONFIGURATION BLOCK

' Data ADO enums
Const adStateClosed = 0
Const adOpenStatic = 3
Const adOpenDynamic = 2
Const adLockOptimistic = 3
Const adUseClient = 3
Dim retVal

' Perform logic to translate configuration to data table identity
Dim sFileType
Dim MSOfficeVersion
Call ADO_IdentifyDataType (sFile, sFileType, MSOfficeVersion)

' Initialization
Dim sComputerName
sComputerName = GetComputerName()
Dim oShell
Set oShell = CreateObject("WScript.Shell")
Dim sScriptResults

(A)
' Run the command
Dim iExitCode, sStdOut, sStdErr
Call ExecuteCommand(sCommand, iExitCode, sStdOut, sStdErr)

' Interpret the results
Dim sStatus, sNotes
Select Case iExitCode
            Case 0
                        sStatus = "SUCCESS"
                        sNotes = ""
            Case Else
                        sStatus = "ERROR"
                        sNotes  = iExitCode & ": " & sStdErr
End Select
' In case there are problems logging, keep going
On Error Resume Next
Call Log_WriteCommandResults(sComputerName, sStatus, sNotes)

(B)
' Modify groups to reflect results
Select Case sStatus
            Case "SUCCESS"
                        retVal= Group_AddMember (sSuccessGroup, sComputerName, & _
                                    "computer")
            Case "ERROR"
                        retVal = Group_AddMember (sErrorGroup, sComputerName, & _
                                    "computer")
End Select
retVal = Group_RemoveMember (sStagingGroup, sComputerName, "computer")
```

associated with document extensions for install on demand. However, publishing Office 2007 means that it isn't deployed until a user needs or requests it, and the user must be an administrator to launch Office Setup, so .zap files also fall short of the deployment requirements for most organizations.

The third option, and the option that Microsoft prefers you use, is to purchase Microsoft Systems Management Server (SMS) or the new rebranded release, Microsoft System Center Configuration Manager 2007. Although SMS and System Center Configuration Manager 2007 provide full-featured support for the deployment and subsequent management of Office 2007 as well as other applications and configuration, they also aren't cheap.

Office Deployment Challenges

As you know, Office 2007 is a large application, typically consuming more than 1GB of disk space, which includes the applications and the local installation source (MSOCache). Installing Office 2007 takes quite a while, so when you're choosing your deployment method it's important to keep in mind how it will impact end users. You don't want your CEO to log on to his or her computer just prior to a presentation to the board of directors, only to find that's the moment when Office 2007 is deployed to his or her system.

Another challenge is that Office Setup requires administrative credentials to execute, so we'll have to develop alternative deployment methods that ensure setup.exe runs with the appropriate credentials. I find it to be rather obnoxious that, in this day of least privilege and non-administrative users, Microsoft didn't provide an easy and full-featured way to deploy Office 2007 using GPSI or logon scripts. Make some noise to Microsoft about this topic by sending an email message to your Microsoft sales representative—the company is developing Office 14 right now.

Most organizations deploy Office to computers, not users. You don't need Microsoft Visio "following" users from computer to computer. It's best to have Office applications installed per machine, available to any user who logs on to that machine. That approach also facilitates license management, since Office is licensed per machine.

With these challenges in mind, let's explore our Office 2007 deployment options. The solutions below will work with both Vista and Windows XP clients in a Windows Server 2003 domain.

The Script

You can install Office 2007 by launching setup.exe. Setup.exe takes optional parameters, as discussed in "Customizing and Deploying Office 2007." If you're launching setup.exe on remote systems to deploy Office 2007, you'll want to ensure that setup finished successfully. Therefore, we'll build a script that not only deploys Office 2007 by running setup.exe but logs its success as well. This script will also ensure that each target system does, in fact, run setup.exe only once. Listing 1 shows a portion of the script, Office2007_Deploy.vbs. You can download the entire script at www.windowsitpro.com, InstantDoc ID 97016. (Click the *Download the Code Here* button near the top of the article.)

Here are the script's core elements:

- The Configuration Block: Office2007_Deploy.vbs is written in VBScript, and you'll find it easy to configure, even if you're not a scripting guru. All required parameters are in the Configuration Block, which is heavily commented to help you understand how to customize the script for your environment. I'll discuss the purpose of each set of parameters a bit later.
- Callout A: The script calls a subroutine, ExecuteCommand, which launches the Office Setup command as defined in the Configuration Block by the variable sCommand (e.g., "\\windomain.com\software\office\sdp\setup.exe"). The ExecuteCommand routine waits for the command to finish, then transfers the exit code and contents of the StdOut and StdErr streams to variables for logging. The code at callout A then interprets the exit code to determine whether the command was successful and calls Log_WriteCommandResults to write a new record to the log.
- Callout B: The script adds the computer to one of two groups (i.e., APP_Office 2007 Deploy or ALERT_Office 2007 Deploy) indicating the success or failure of the command and removes the computer from the staging group (i.e., CMM_Office 2007 Deploy). I'll explain these groups in more detail shortly.

To use the script, save it to your Office 2007 network installation point. I suggest creating a folder at the same level as setup.exe and the Updates folder called CompanyName_Setup. Put the script in that folder and secure the folder so that Authenticated Users have Read permission, and only administrators have Modify permission. Because the script will be run on systems using administrative credentials, you don't want untrusted users to be able to modify the script.

Don't forget to put your Office Setup customization file in the Updates folder and to use the /adminfile switch on setup.exe to point to the Setup customization file. Your Setup customization file should ensure a silent installation of Office 2007. (For more information about how to point to your Setup customization file, see "Customizing and Deploying Office 2007.")

The Log

The script logs the success or failure of the setup.exe command after the command is executed on each system. You must create a log file. The script is coded to work with a Microsoft Excel worksheet (Excel 97–2003 .xls format) as the log file, although you can change the script to work with a log file in the form of a Microsoft Access database (.mdb), Microsoft SQL Server database, or Office 2007 format database (.xlsx or .accdb). If you create an Excel worksheet, you'll want to create column labels in the first row that match the labels defined in the script (i.e., ComputerName, Action, Status, Date, Notes). If you rename the worksheet from the Excel default name, Sheet1, remember that you must change the sTable variable in the script. Save the script to a folder to which Authenticated Users have read, execute, and write permission, and configure the variable sFile to point to the database.

The Groups

You can use the log to audit the success and failure of setup.exe, but it's also handy to be able to easily monitor the machines on which Office should be installed, those for which setup.exe succeeded, and those that encountered errors. To do so, leverage Active Directory (AD) as your database and create the following three global security groups in AD:

- CCM_Office 2007 Deploy: This group will contain the computers to which Office 2007 will be deployed.
- APP_Office 2007: This group will contain computers on which Office 2007 has been successfully installed.
- ALERT_Office 2007 Deploy: This group will be used to flag computers on which Office 2007 deployment failed. You can then monitor this group's membership to determine which systems might need support.

The benefit of using AD as a database is that doing so makes it easy to manage change using group memberships. Computers in the CCM_Office 2007 Deploy group (CCM for Change and Configuration Management) will run the script using the methods described below. When the script succeeds, it moves the computer into the APP_Office 2007 group. If the script fails, it moves the computer into the ALERT_Office 2007 Deploy group. With either success or failure, the computer is removed from the CCM group, so that the script doesn't run repeatedly.

For the script to move the computer between groups, you must delegate these groups correctly. These groups require the Self Allow Write Members permission. With this permission, the special identity Self must be allowed to modify the Members property. A user (or computer) can add or remove itself from a group but can't add or remove other members. You can configure this access control entry (ACE) in the Security Properties dialog box of each group or place these groups in an organizational unit (OU) delegated with the Allow Self Modify Members ACE.

This ACE can be delegated on the OU. To do so, open the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in and select Advanced Features from the View menu. Then, right-click the OU containing the three groups and select Properties. Now, click Advanced under the Security tab. Click Add and enter SELF for the User or Group. Then click OK. In the Permission Settings dialog box, click the Property tab and select Group Objects from the drop-down menu. Now select the Allow check box for the Members property.

Group Policy Startup Script

Although GPSI doesn't support Office 2007's setup.exe command, startup scripts can execute any command you want to run. Startup scripts run locally in the context of the System identity, which provides sufficient access to run setup.exe successfully.

The Microsoft article "Use Group Policy to assign computer startup scripts for 2007 Office deployment" (technet2.microsoft.com/Office/en-us/library/a57c8446-b959-4025-a866-b690ddcaa66d1033.mspx) describes how to use startup scripts for Office 2007 deployment. Although the article is strong on concepts and on step-by-step instructions for creating and assigning startup scripts, the actual script it proposes is weak. Our script is much more robust.

There are two things to keep in mind if you decide to use startup scripts to deploy software.

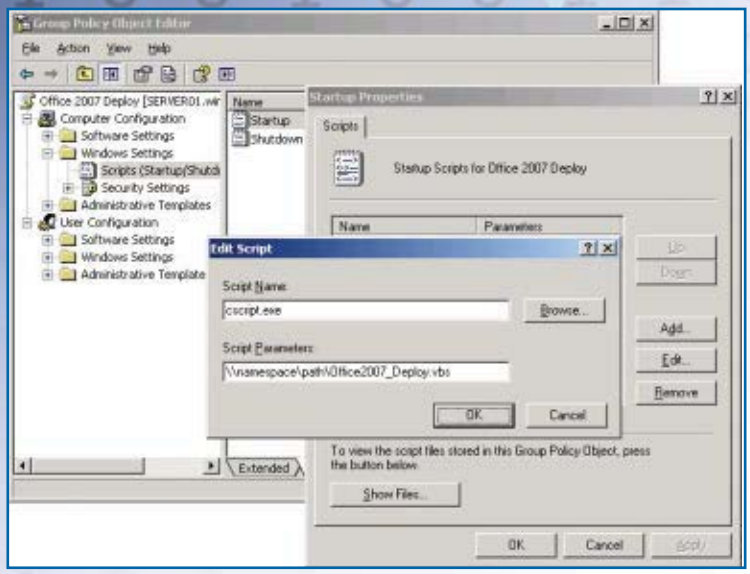


Figure 1: *Editing the GPO Startup Script policy settings*

The first is the length of time it takes to perform the installation. Startup-script processing times out after 10 minutes by default, so you'll need to match the script timeout Group Policy Object (GPO) setting located under Computer Configuration\Administrative Templates\System\Scripts*Maximum wait time for Group Policy scripts* with the maximum time (in seconds) that's required to install Office. Determine the time through testing, but 15 to 20 minutes (900 to 1200 seconds) should be enough. I recommend configuring the expanded script timeout in the same GPO that you use to deploy Office, so that when the GPO no longer applies to a computer, its script timeout will return to the default or to another setting configured by other custom GPOs.

The other thing you must keep in mind when using startup scripts is how it will impact your end users. Startup scripts will run at each system startup, so you don't want to be running setup.exe every time a client computer is booted. Setup won't reinstall Office—it will detect the existing installation successfully—but it will still take time to process. Therefore, you want to configure your startup script to verify whether Office 2007 already exists on the system prior to running setup.exe. If Office 2007 has already been installed, the script will exit without running setup.exe.

There are several ways to configure your startup script to verify whether Office is already on a system. One way is to read the registry key that displays Office 2007 in the Add/Remove Programs list. If it's there, Office 2007 is installed. Another method is to create your own registry entry to track the successful installation of Office 2007. I'm a big fan of tagging systems for CCM. You can also create a "flag file" on the hard disk. Many systems administrators use this approach to tag a system. An empty text file is created with a specific name such as C:\OfficeDeployed.txt. A script looks for this file to determine whether the script should run. I prefer to use a registry change rather than the flag-file method, since disk reads are more "expensive" than registry reads from a processing perspective, and there's a risk of the file being deleted from the disk.

Finally, you can use a security group to deploy Office 2007. To do so, create a GPO called Office 2007 Deploy. This GPO will configure the startup script, which will install Office 2007. Edit the GPO Startup Script policy settings to run your script: The Script Name should be cscript.exe, and the Script Parameters should be the full path to your script in the Office network installation point, as Figure 1 shows. Try to avoid using spaces in the pathname or filename.

After you've created the Office 2007 Deploy GPO with the startup script that installs Office 2007, filter the GPO so that it applies to only the CCM_Office 2007 Deploy group, as Figure 2 shows. Don't forget to remove Authenticated Users from the filter.

Any computer that's in the CCM_Office 2007 Deploy group will run the startup script and install Office 2007. Now here comes the creative part. Because the startup script includes code that removes the computer from the group, the startup script will run only one time on that computer. Also, if Office installs successfully, the computer will be moved to the APP_Office 2007 group. You can use that group to monitor and report which computers have Office 2007. If Office installation fails for some reason, the computer will be added to the ALERT_Office 2007 Deploy group, which acts as a "red flag" for computers that should be examined to determine why Office installation failed.

Wrapping Up

We've created a script that acts as a "build-it-yourself" SMS or Systems Center Configuration Manager by executing an action, logging the results, and ensuring the action doesn't happen again. We've also looked at how to deploy the script by using Group Policy startup scripts. For more information about other Office 2007 deployment methods, see the Web-exclusive sidebar "Alternative Office 2007 Deployment Methods," InstantDoc ID 97263. The approach I've laid out can be used for several systems management tasks in addition to deployment of Office 2007.

InstantDoc ID 97016

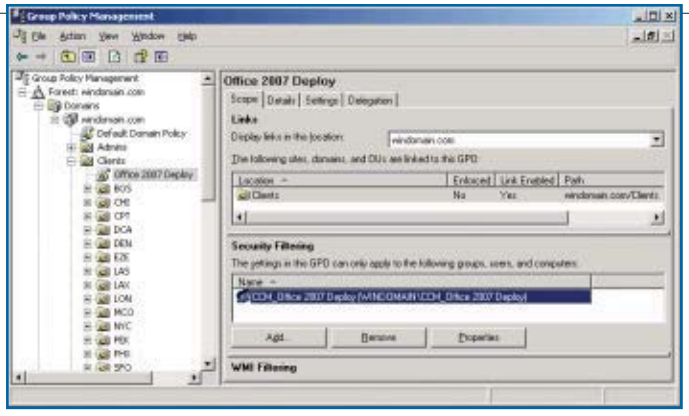


Figure 2: *Filtering the CCM_Office 2007 Deploy GPO to apply to only the CCM_Office 2007 Deploy group*

Dan Holme
(danh@intelliem.com) is director of consulting at Intelliem, which delivers solutions-focused training and consulting services supporting enterprise SharePoint, Office, Windows, and Active Directory implementations.

Stsadm: Taking Control of SharePoint Administration

Use this command-line tool to customize and automate SharePoint management

by Kevin Laahs

Each new version of SharePoint has brought changes in the options for managing it via a graphical UI. The current versions of SharePoint—Windows SharePoint Services (WSS) 3.0 and Microsoft Office SharePoint Server (MOSS) 2007—provide a Web UI called Central Administration. This application lets you manage the SharePoint farm at different levels—from individual services on servers to Web applications to shared services.

However, some operations, for example changing the schedule of a background task or setting the diacritical sensitivity on a search index, aren't exposed through the UI. To perform such operations, SharePoint administrators need to call upon the stsadm .exe command-line utility. Let's look at what Stsadm is, some of the operations it supports, and how you can use it to automate common management tasks.

Stsadm helps IT pros perform operations that can't be done through Central Administration.

Stsadm

Stsadm has been shipping with SharePoint products since its inception. It helps IT pros perform operations that can't be done through Central Administration and automate and batch operations that would take longer to complete using the Web interface. Indeed, the tool's name alone gives us a clue to how long it's been around: The first real SharePoint offering was called SharePoint Team Services (STS), and it primarily was managed via Stsadm.

Each SharePoint release has significantly extended the operations that Stsadm can perform, and today, MOSS has 183 operations that the utility can perform. You can extend the functionality of Stsadm by adding other operations to it, which is useful for third parties that layer applications on top of SharePoint. It's also useful for extending the base capability of SharePoint. You can find information about how to extend Stsadm in the Windows SharePoint Services Software Development Kit (SDK) at www.microsoft.com/downloads/details.aspx?FamilyID=1c64af62-c2e9-4ca3-a2a0-7d4319980011&displaylang=en.

You'll find Stsadm on any server that has had either WSS or MOSS installed on it. It's located in the \%ProgramFiles%\Common Files\Microsoft Shared\web server extensions\12\BIN\ folder. That's a long path to have to navigate to whenever you want to use Stsadm, so the first thing I recommend is to set up a command prompt short cut that starts in this folder. Note that to run Stsadm, you must be a member of the local Administrator's group on the server.

You control what each operation does by passing it relevant parameters. You can see the syntax for each operation by opening a command line and typing

```
stsadm -help <operation>
```

You can dump the list of all operations by using Stsadm with no parameters. Microsoft provides more information about Stsadm at technet2.microsoft.com/Office/f/?en-us/library/5beaaf55-b77c-442d-88f5-eb9672f82e661033.mspx and technet2.microsoft.com/windowsserver/WSS/en/library/2c5896ac-edf6-4c2d-b750-995bbb66909c1033.mspx?mfr=true and via the WSS and MOSS SDKs, but the information isn't complete. Therefore, trial and error may be required to achieve the desired result. You can also find documentation for commands that aren't available from the UI at technet2.microsoft.com/Office/en-us/library/188f006d-aa66-4784-a65b-a31822aa13f71033.mspx?mfr=true.

The output of an operation will differ for each operation and may or may not be useful for automating common management tasks. For example, the enumsites operation, which enumerates the site collections in a Web application, produces XML output that you can subsequently parse to perform mass management tasks on all site collections. Figure 1, page 70, shows the site collections that were enumerated from a Web application whose URL is moss.spysrus.com/. Attributes within each XML node provide further information, such as the content database and storage limits associated with each site collection, so you could use this functionality to move all the site collections in one content database to another.

5 Favorite Stsadm Operations

It would be impossible to go through all 183 Stsadm operations, so here I highlight five of my favorites. I selected these operations

Learning Path

WINDOWS IT PRO RESOURCES

Learn about SharePoint:

"SharePoint Server 2007 Revealed," InstantDoc ID 94914

Learn about SharePoint and Stsadm:

"Bridge the SharePoint File-Restore Gap," InstantDoc ID 93239

"Get Past the Gaps in SharePoint," InstantDoc ID 48919

MICROSOFT RESOURCES

Stsadm command-line tool (Office SharePoint Server)
technet2.microsoft.com/Office/en-us/library/188f006d-aa66-4784-a65b-a31822aa13f71033.mspx

Welcome to the Microsoft Office SharePoint Server 2007 SDK
msdn2.microsoft.com/en-us/library/ms550992.aspx

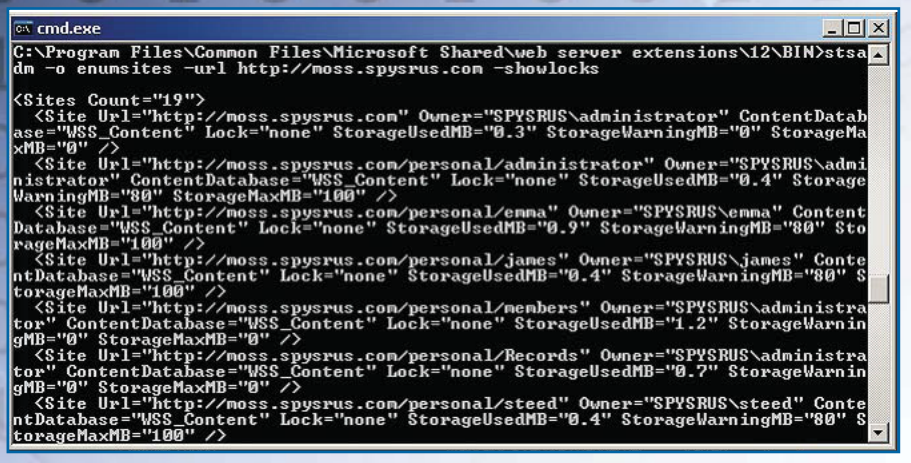


Figure 1: *Using Stsadm to enumerate site collections*

because they're likely to be used in most SharePoint installations.

MigrateUser. When a user is granted access to a site collection, certain details about the user are written to the UserInfo table in the back-end Microsoft SQL database. One such detail is the user's SID, which ultimately controls access to the site collection. Should the user's SID change for any reason—for example, if his or her AD account is moved to a different domain—the user loses access to existing site collections because the old SID is still in the database. You can use the migrateuser operation to fix the problem. This feature reads the old and new logon details and updates the relevant details in the database.

Createsiteinnewdb. Every site collection exists in only one content database. By this I mean that all the content from all the sites and subsites within the collection are stored in the same database. When you create a site collection through the UI or through the createsite operation in Stsadm, the content database that houses the collection is the one that is currently least full in terms of the number of site collections that it can host. The createsiteinnewdb operation is especially useful for situations when you want to target a particular site to a particular content database—for example, certain sites may have particular service level agreements (SLAs) associated with them and are therefore stored on separate SQL servers.

Backup. The backup operation lets you back up individual site collections as well as the entire farm (including search indexes) to disk. The ability to back up site collections is useful if you have crucial sites that need to be backed up more frequently than your regular backup. You can create a single file that contains everything within a site collection, and you can automate the backup through a scheduled recurring task. You can also use the export operation to produce a backup file that doesn't contain the full contents of the site collection or farm. For example you can omit item versions, thus reducing the size of the backup file.

Restore. Of course having a backup of a site collection is pretty useless if you can't restore the site collection if need be. The restore operation can take a file created using the backup operation and restore a full fidelity copy of the site collection, either by overwriting the existing site collection or creating a brand new site collection. This operation is useful for making copies of site collections for testing/debugging purposes (e.g., copying a production site collection to a test or staging farm).

SetProperty. The setproperty operation, along with its counterpart getproperty, is used to set attributes on many different SharePoint components. For example, you can use the job-usage-analysis property to control the frequency and time of day for usage-analysis processing on the server. Similarly, there are properties that control the frequency and time that the server sends out alerts. You can see a list of the configurable properties by typing the command

```
stsadm -o setproperty
```

A partial list of documented properties is available at office.microsoft.com/en-us/winsharepointadmin/HA011608451033.aspx.

There are many SharePoint timer jobs that you can view using the Operations tab from SharePoint Central Administration. You can also see the frequency of each job, but Central Administration provides no way to change this frequency or the time of day that the timer job runs. As I mentioned earlier, some jobs are controlled via a configurable property, but others are controlled via their own operation. For example, there are operations for controlling when the information management expiration policy runs (setpolicyschedule) and when profile synchronization occurs (setsearchandprocessschedule). These operations take a "recurrence string" as a parameter (e.g., "every 10 minutes between 0 and 59" or "daily at 13:00"). Therefore, if you need to kick off a task immediately, you use Stsadm to tweak its schedule. To find out what the syntax for using these recurrence strings are, look at the Help for setcontentdeploymentjobschedule.

Using Stsadm to Automate Tasks

Because Stsadm is a simple command-line utility, you can further simplify its use by wrapping it in a script or command file that can take parameters. You can also use the Windows Task Scheduler to schedule common tasks you perform with Stsadm. For example, you can schedule regular backups of particular site collections by placing the appropriate backup operations in a command file and scheduling the file to run at the appropriate times.

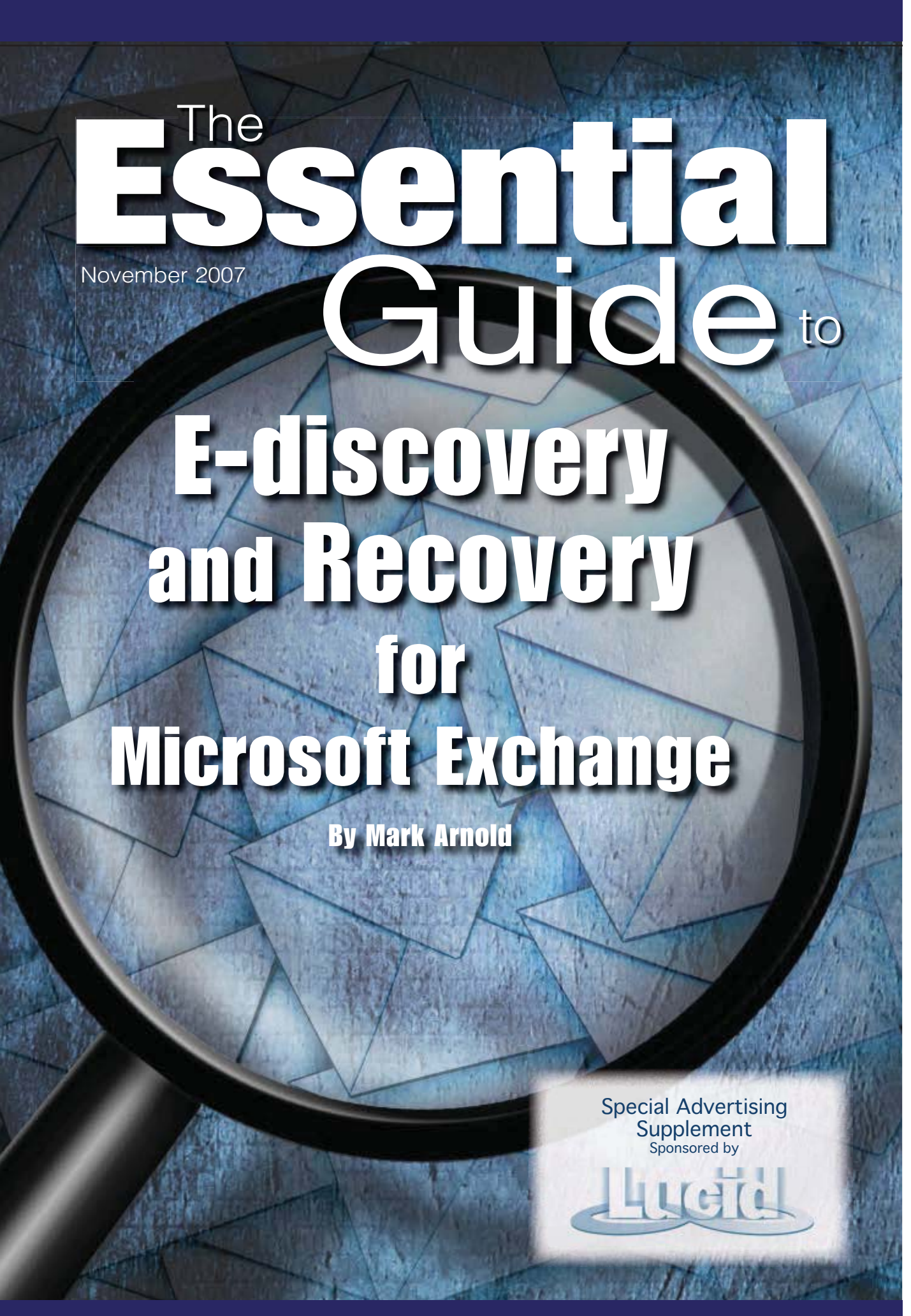
You can also leverage the output from some Stsadm operations. A simple example here is the enumsites operation that I mentioned earlier and its companion operation enumsubwebs. These output XML files are convenient fodder for many Web Parts. Therefore, if you schedule a task that enumerates your sites and directs the output of that task to a central file, you can use that file as input to a Web Part to display your up-to-date list of sites in a Web Part page.

Leverage the Command-Line to Extend SharePoint's Web-Based Management

Stsadm is the SharePoint administrator's friend. Whether you want to automate standard operations or perform tasks that are not so common, you can turn to Stsadm. If you haven't already done so, I urge you to fire up that command prompt and see what Stsadm can do for you.

InstantDoc ID 97107

Kevin Laahs
(kevin.laahs@hp.com) is a principal consultant in the HP Services Advanced Technology Group. He is coauthor of *Microsoft SharePoint Technologies: Planning, Design, and Implementation* (Digital Press).


The
Essential
Guide to
E-discovery
and Recovery
for
Microsoft Exchange
By Mark Arnold
November 2007
Special Advertising
Supplement
Sponsored by
Lucid

With more than 75 percent of business-critical information residing in e-mail today, you are more likely to find evidence sitting in someone's inbox than in their filing cabinet or on a file share. The growing importance of e-mail has not been lost on the lawyers, courts, or government regulators. In fact, e-mail is being placed at the center of legal discovery requests and is increasingly used in a variety of legal and regulatory proceedings, from e-discovery for civil lawsuits to providing the grounds for prosecuting criminal cases. For example:

- According to IDC, 27 percent of fortune 500 companies have had to deal with harassment claims concerning e-mail.
- The ePolicy Institute found that 21 percent of companies surveyed were required to produce employee e-mail in legal cases.
- According to a recent study conducted by Osterman Research, a typical organization conducts 14 searches through e-mail each year for legal discovery.

What's at stake?

The failure to provide a complete record of historical e-mail information, when requested to do so, can be an expensive business. A survey in 2004 of 840 U.S. companies by ePolicy Institutes revealed that some 80 percent of respondents had been subpoenaed to provide e-mail or Instant Messaging communications in support of legal action. Two high-profile cases illustrate the point:

- Morgan Stanley was fined $1.45 billion in 2005 for deleting and failing to provide e-mails in advance of pre-trial discovery. While an extreme case, it does show that penalties in this area are potentially very high.
- In the case of Bank of America Corporation vs. SR International Business Insurance Company 2006 WL 3093174 (N.C. Super. Nov. 1, 2006), the defendants requested that a non-party to the case produce deleted e-mails from 400 backup tapes. The estimated cost to produce these e-mails was $1.4 million, or an average of $3,500 per tape.

Clearly, IT managers need to be acutely aware of the risks that a business faces when asked to disclose information to external investigators or auditors. In this Essential Guide, we will present some of the regulatory and technical challenges that a business faces and the ways in which an IT department may approach recovery and discovery requirements in an integrated manner.

Ever More Regulations

On December 1, 2006 amendments to the Federal Rules of Civil Procedure (FRCP) changed the rules regarding management of electronic stored information (ESI) for all organizations that operate within the United States. These changes defined such things as the role of electronic messaging where litigation is pending or in progress. When it comes to regulations, companies have to assess their exposure and make a choice about whether the organization is required to retain e-mail for a period of time that forces consideration of an archiving solution, or whether the necessary backup retention period means that they can properly manage their recovery procedures to provide the required discovery items whenever needed.

When addressing that question organizations should further assess whether or not they are required to produce messages deemed not to have been tampered with. Even if the business is not required to retain messages for several years it may still be required to retain messages in a "forensically secure" manner, which is not something Exchange can do on its own. If there is a requirement to produce messages that cannot have been modified or tampered with in any way, then an external solution, completely outside of Microsoft Exchange, is necessary.

While many organizations have decided that they must comply with the tightest interpretations of regulations such as HIPAA, SOX, FRCP, and others, many more businesses have no need to secure messages in a dedicated e-mail archive system. Instead, they rely on their backups and then restore and extract the required information from them when a discovery request comes in. A simple cost-benefit analysis is conducted to weigh the cost, including software, hardware and maintenance, of using a fully blown archiving product against the cost to the business of maintaining backup tapes or on-disk storage for as many backups as is required. While it is appropriate for many businesses to procure solutions such as Symantec Enterprise Vault and Zantaz EAS, some businesses simply have no need to archive e-mails in a near-line storage system for an extended period of time. The flowchart (Figure 1) shows a simple decision process to determine whether a full archiving product is required, along with recovery management tools, or whether a business would meet its obligations by using recovery management tools alone.

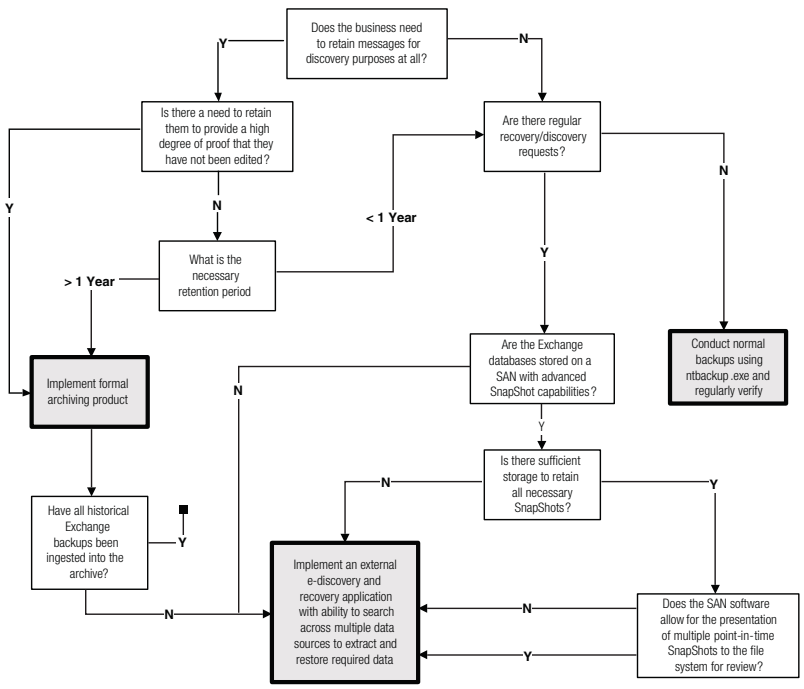


Figure 1 *Decision Flowchart*

The Halcyon Days

Only a few years ago life with e-mail was simpler. You backed up your Exchange server and you prayed your tapes worked in case you needed to restore the server. Then someone decided it would be a good idea to be able to restore individual messages. Backup vendors, always good at making a backup solution but not necessarily good at providing a seamless restore experience, came up with a new and not entirely reliable method to do this by taking a second pass at the Exchange database or Information Store via MAPI for Brick-Level Mailbox Backups. This approach used up lots of extra tape space and even on a relatively small database would take a very long time. Anyone with stocks and shares in tape manufacturers was instantly very rich indeed.

Today, vendors are beginning to introduce single pass offerings which can help with single-item restores (if you know where the item is located) but do nothing to help with search or discovery requirements.

Matters became more complex when businesses started using their e-mail systems as the authoritative source of information. Legal departments very quickly realized their exposure to this medium and began asking how they could prove that messages were received or sent, or what action was taken on a particular message and other important actions in the business process. The market for archiving and discovery products emerged to fulfill these ongoing, complex, and evolving needs.

Some applications offer one of those two capabilities (archiving or discovery); some offer both or integration between archiving and discovery applications. However, none of these applications can extract data directly from the backup of an Exchange database. The point here is that two distinct categories of application haven't tended to overlap, so there are often differing ways to get at the same information. It is self evident therefore that there is a very clear requirement for an application that can open a backup copy of an information store to do both item-level restore and discoveries where required.

Today the Microsoft Exchange e-mail archiving market is relatively crowded. Many different applications offer a wide range of features, but they all tend to boil down to two, rather catch-all features that can significantly increase the amount of storage taken up. The first type is Journaling which, by necessity, captures every single message coming into the organization—including spam and other potentially inappropriate content that would otherwise have no place on your corporate network. The second is best described as Threshold/Policy Based archiving, where messages for a group of mailboxes or items over a certain size or age are removed/stubbed from the information store into the archive. The obvious benefit here is that Threshold/Policy Based archiving allows for the customization of the archiving rules to fit the needs and governing policies/regulations of the organization. The downside, however, is that the archive can very easily miss messages that are forcibly deleted by mailbox management rules or by the user after sending or receiving. It does not matter whether the deletion was done for legitimate or nefarious reasons. The point is that the message is gone. Some of you may be thinking that you can always restore the item from backup. If you are protecting the data via once-a-day tape backup, the message is gone forever. If you are using snapshot technology, you might be able to recover the information if a snapshot took place before the deletion. In the event that a Continuous Data Protection application is in use, the deleted message will be captured so that a recovery application can extract it. But the bottom line is that no matter what backup solution is in use, the data will never reach the archive. Certainly, items that never reach the archive will be the very ones you actually need to produce.

Archiving solutions have the ability to ingest PST files that most likely are littered across your network. However, they cannot extract and then ingest information from previous Exchange backups. A superior solution is to have a product that delivers a space-efficient and flexible electronic discovery method providing auditors and investigators a simple-to-use interface to search and extract the required information directly from legacy Exchange backups, snapshots, or CDP repositories. This information can then be restored, utilized for required discovery purposes, or ingested into the Archive.

How are messages recovered?

It is all well and good having made the decision that an archiving solution is or is not required, but what are you going to do if presented with a request to recover e-mails that span a period of months or years and you only have backup tapes or files to work with? The conventional way would be to restore each information store that you want to search through into the Exchange Recovery Storage Group (RSG) and use Exmerge to search through the store against the necessary parameters such as recipients, dates, and subjects in order to extract the messages you need. Once you have done one store you then have to restore another backup and start all over again. One of the major problems with this approach is that e-mail cannot be extracted from a deleted account using the RSG. Therefore, you can never delete any Active Directory (AD) account that had an associated mailbox.

Another often-used method is to use a parallel/recovery infrastructure and restore each database along with a copy of AD that contains the accounts available at the time of the backup. Execute the search much like you would with the RSG and then extract each mailbox into a PST. Luckily, with this methodology you are able to delete defunct accounts within your production infrastructure so your AD remains yours to manage the way you want. As you can see, this may be satisfactory for two, perhaps even three backups, but beyond that the time taken and the possibility for error make this approach unsustainable.

With either methodology, once you have all the required mailboxes extracted to PST format you will soon discover that searching through those multiple PSTs—as well as the text within attachments—in order to de-duplicate and extract a consolidated data set

simply isn't possible. Very quickly it becomes obvious that a powerful search tool, capable of looking through multiple information sources to discover, de-duplicate, and recover the required information is critical.

Networked Storage

With the advent of iSCSI Storage Attached Networks (SANs), the use of tape as the primary recovery medium has been waning. SANs have the excellent advantage of being able to provide SnapShot backup capabilities and those backups are retained on disk for a period of time. The amount of time the backups are retained is primarily a budgetary factor because although they are efficient, SnapShot backups are not entirely cost-free in terms of physical disk utilization. Where the SAN does provide administrators with a positive advantage is that they have the ability to present the raw Exchange database files from previous points in time.

These SnapShots work best when they are carefully managed and purged as their retention becomes redundant. Hourly backups are replaced by daily backups, which are eventually replaced by weekly backups. These SnapShot backups remain on disk where the SAN software mounts them in virtual Logical Units (LUNs). Windows sees them as complete files that may be worked with as if they were individual, multi-gigabyte, information stores. A SnapShot backup may appear to the operating system as a full 70GB information store, but it may take up only a small fraction of that space on disk.

If a recovery or a discovery request can be met without having to wait for tapes, that can only be a good thing for IT departments. It means their Service Level Agreements (SLAs) for recovery and discovery can be met and that they also can reduce the skill level required to conduct the restore or discovery. What used to take a tape-based restore and the expertise of an Exchange administrator can now be done by a helpdesk operator working to a script. Any task that releases well-paid resources to carry more challenging activities helps staff retention and morale. Of course, having access to the SnapShot backups is only part of the story; there still needs to be an application, such as Lucid8's DigiScope, that can open those SnapShots to search, extract, or recover information. No native solution from any SAN vendor can do this in isolation.

Handing over the information

Just because you use Microsoft Exchange and Outlook it does not follow that the same platform is being used by the people to whom you are providing the information. Burning a PST file onto a DVD is not necessarily going to be a format the receiver will be able to use. A PST file is limited in size and renowned for being prone to corruption. Remember that there are now two PST formats and a PST generated within Outlook 2003/2007 cannot be read by Outlook 2002 (XP) and earlier. It is no longer a case of just providing a PST and knowing that it's readable—assuming it doesn't become corrupt along the way. A sensible approach then, is to have the ability to provide the required information in a manner very much less likely to suffer from corruption problems and in a format that works best for the requestor. When you evaluate combined recovery and discovery applications, make sure that high on the list of success factors is the ability to read from and export to both PST formats as well as export data into other readily acceptable formats such as MSG, XML, and others.

Is there a better way?

When a backup vendor provides a way of getting single messages out of a backup they tend to do so in such a way that only a single backup can be opened at any one time.

Few applications will open raw Exchange database files. Even fewer applications possess the capability to open, search, and extract data from multiple copies or data sets of raw Exchange database files as well as PST files. Using an application that gives you the opportunity and power to carry out these actions from a single interface as well as conduct any required mailbox or item level restores is of great benefit to your business.

As stated earlier, even organizations that have deployed e-mail archiving systems at some point may need to restore backups in order to retrieve required information that has not made it into the archive. It is neither a common practice nor an easy task to import the data from backup tapes into an archive.

Whether your organization implements an e-mail archive or not it's clear that the IT department needs the ability to efficiently search, export, and recover e-mail related data directly from Exchange database backups in response to any ad-hoc discovery or recovery requests.

Let's take a common scenario. The organization for which you work is not subject to strict data retention regulations but does need to provide discovery capability for messages sent and received in the past six months to a year or so. At the same time, the organization has decided to ensure that all messages over a certain age are purged from the running Exchange information stores beyond 60 days by using the standard Mailbox Management Recipient Policy. The organization likes to maintain the AD in a well-managed state, deleting user accounts as soon as employees leave. This provides the IT department with a dilemma on how it may provide not only normal recovery actions but also discovery requests for individual items or mailboxes of ex-employees as well as active user accounts.

By using the standard Windows backup application (ntbackup.exe) to restore any required information store database files, to a standard directory structure with the "restore to alternate location" option, an administrator can have an extensive history of e-mail at his disposal to search through. By using the most basic of backups the administrator gives himself the ability to concentrate on using a feature-rich e-discovery and recovery solution. Remember, a backup isn't about backing up something, it's all about how a recovery can be handled should it be necessary. Keep the backup simple and give yourself the flexibility to recover in the most appropriate manner. No Microsoft application has the ability to take multiple restored file types, mount them into a single application, and conduct a search across them. And remember that even though you can restore and mount a single database into the Recovery Storage Group you still can't recover

individual items or search through one or more Exchange databases in an effective manner. Choosing an e-discovery and recovery application that allows such functionality has several benefits for the business and for IT:

- You can run the production Exchange server using smaller databases, which back up faster and are quick to restore should a conventional "disaster" occur (e.g., multiple disk failure or store corruption)
- You can concentrate on performing database backups only rather than database and mailbox backups (which are problematic, take more time, overhead, and resources)
- You can reduce or even eliminate any space allocated to the Recovery Storage Group, thus keeping the storage allocated to the Exchange servers lean-and-mean
- You can use a standard workstation class machine with inexpensive storage as the recovery server rather than a server with the faster, invariably smaller, and always more expensive SCSI disks
- By doing backups to disk and then sending the backup files to tape, you can readily access the most up-to-date information on the fly. And you can send the tapes off-site knowing that you are unlikely to need them back (which does not, of course, abrogate the responsibility to test the tapes before they go off-site)

The decision is yours

Applications that archive e-mail, whether with simple archiving in mind, or for the express purpose of providing extensive discovery, are invaluable to those businesses that are subject to the most stringent retention regulations. Those organizations that don't have to provide seven or more years' worth of documentary evidence may still be subject to regulations that require them to provide information upon request, but to a far more relaxed degree of proof.

By taking a view of exactly what the retention, discovery, and recovery requirements are, a business can choose the appropriate archiving solution or a simple, basic backup utility to protect its Exchange servers. Regardless of your selection be sure to deploy a powerful application in conjunction with archiving or simple backups that provides database, mailbox, and message recovery capability—as well as any message discovery that may be necessary.

Mark Arnold, MCSE+M, Microsoft MVP, is a technical architect for Anix, a UK-based storage integrator. He is responsible for the design of Microsoft Exchange and other Microsoft Server solutions for Anix's client base in terms of the SAN and NAS storage on which those technologies reside. Mark has been a Microsoft MVP in the Exchange discipline since 2001, contributes to the Microsoft U.K. "Industry Insiders" TechNet program, and can be found in the Exchange newsgroups and other Microsoft Exchange forums.

A Single-Search Solution

DigiScope from Lucid8 offers a single interface that allows administrators to conduct a single search, as shown in Figure A, through multiple sources such as:

- Production information stores
- Exchange backups restored to alternate locations
- Mounted SAN-based volume snapshots
- DigiVault Continuous Data Protection (CDP) repositories

Once all the data sources have been presented to the management interface the administrator may run searches for either user restore requests or in response to discovery compliance instructions. Mailboxes, folders, conversation threads, or individual messages may be restored from a backup to the production store by simple drag-and-drop process or extracted from the backups into multiple file formats, including PST files so that the information may be taken by investigators.

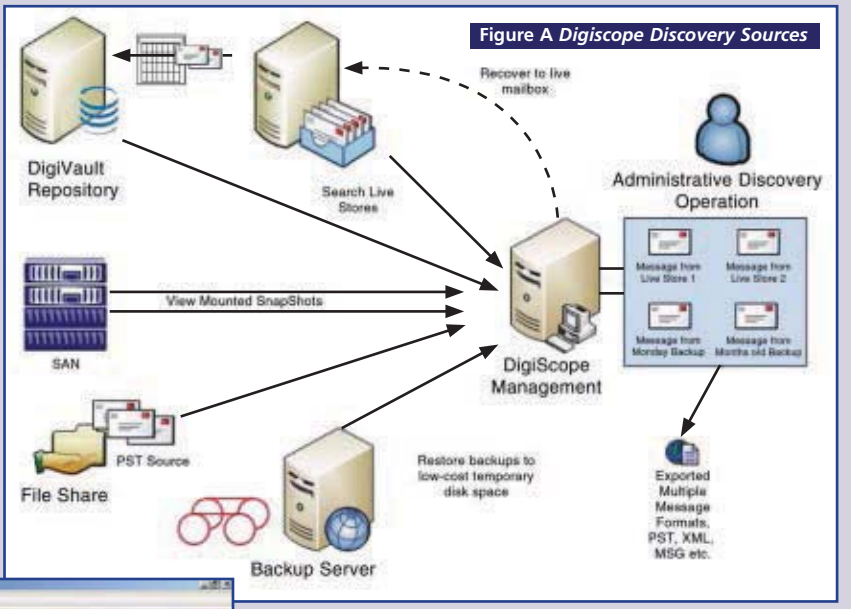


Figure A *Digiscope Discovery Sources*

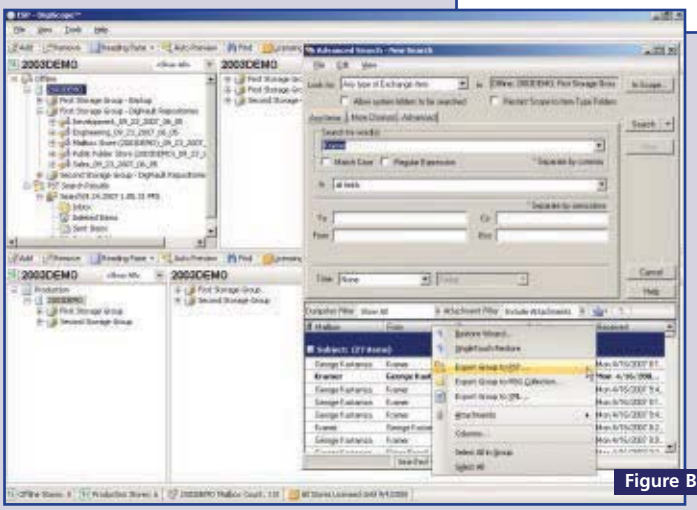


Figure B *DigiScope Recovery Console*

Figure B shows the DigiScope interface and how it allows you to interrogate several types of media with a single query and provide an integrated view of the results.

It's Not Just E-mail, It's Evidence

DigiScope

E-discovery and Recovery for Exchange

The Federal Rules of Civil Procedure (FRCP) require organizations to manage their e-mail in such a way that it can be produced in a timely, complete and viewable manner. This and the fact that more than 75 percent of business-critical information resides in e-mail today reflects the stark reality that e-discovery and recovery of e-mail is now a routine, yet critical, aspect that every organization must address.

• DISCOVER • RECOVER • RELAX

DISCOVER – DigiScope's robust and flexible search capabilities enable you to rapidly query one or more Exchange databases, PST files, or DigiVault® data sets to locate a specific mailbox, folder, e-mail item, or entire conversation thread in record time.

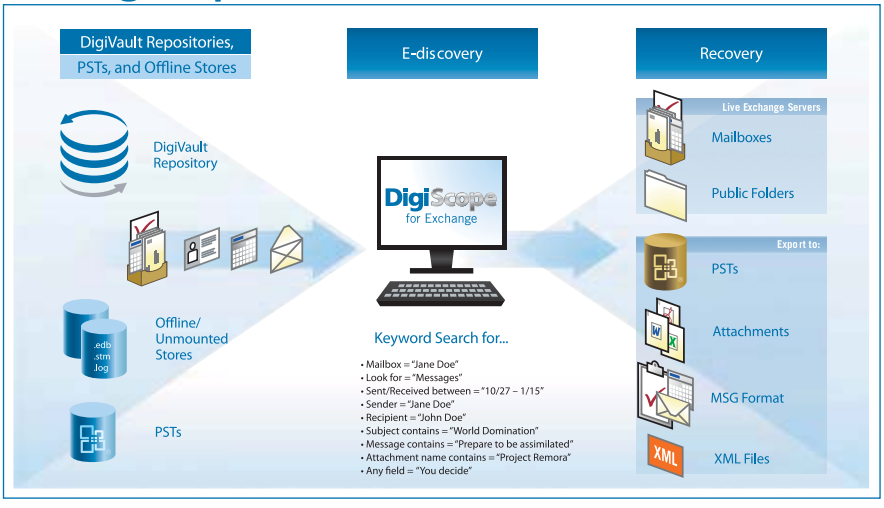
RECOVER – Easily restore individual mailboxes, folders, messages, contacts, schedules, and other e-mail items directly to your production Exchange server, or extract the required data into a PST, MSG, XML, or native attachment file format for transport, review, regulatory compliance, or Legal hold.

RELAX – With DigiScope, you can quickly find and recover invaluable lost, deleted, or historical data without implementing never-ending mailbox brick-level backups, costly Exchange recovery infrastructures, or ineffective Recovery Storage Groups.

Created by Lucid

Solutions Inspiring Confidence

How DigiScope Works



FREE DOWNLOADS

- Demo version of DigiScope
- White Paper –"The Federal Rules of Civil Procedure, E-mail Discovery and You." by Osterman Research

Go to: www.Lucid8.com/ESGdiscovery
Call: 425 456-8496
E-Mail: Sales@Lucid8.com

Q: I have several software packages that were deployed using Group Policy Software Installation. I want to retire the server that houses the packages I've deployed, but if I move the packages, this will trigger a reinstallation of all the applications that have already been deployed. Is there any way to get around this?

A: This is a common problem with no easy solution, but I'm asked about it so often, it deserves an explanation. The first thing I'll say is that I always recommend that when you use the Software Installation feature in Group Policy, that you deploy your packages from a DFS or DFS Replication (DFSR) share. Doing so gives you the flexibility of moving the physical package from server to server without requiring a change to the package's logical path. That being said, if you're in this situation, there's little you can do out-of-the-box to repoint an already-deployed package to a new location. There are several reasons why this is difficult. The first is that the package path location is embedded both within the Active Directory (AD) portion of the package definition within a given Group Policy Object (GPO), as well as within a package advertisement (.aas) file in the SYSVOL portion of the GPO. You can't simply modify the .aas file because it's a binary file that's generated when you deploy the package. The problem gets even more difficult if you've deployed transforms as part of your installation because transforms are cached by the client during installation and are never recached as part of a redeployment. Finally, the client keeps information about the path to the package in its registry, and changes to that path will "orphan" the application for future modifications, upgrades, or patches. So make sure you deploy your packages from a DFS or DFSR share and avoid the problem.

There's little you can do to repoint a deployed package to a new location.

InstantDoc ID 97121

—Darren Mar-Elia

At a Glance

Q: How can I convert an ADM file into an ADMX file?

A: Prior to Windows Server 2008 and Windows Vista, Group Policy templates were created in Microsoft's proprietary ADM format. With Windows 2008 and Vista, Microsoft has switched to a new XML-based format, ADMX. You can use Microsoft's ADMX Migrator tool to convert custom ADM files to ADMX. You can download the tool at www.microsoft.com/downloads/details.aspx?FamilyId=0F1EEC3D-10C4-4B5F-9625-97C2F7310900&displaylang=en. The tool also includes an ADMX editor that makes creating customized ADMX files much easier.

To convert an ADM file, open the ADMX Migrator Command Window and run the faAdmcConv command. For example, to convert blocksharecreate.adm, I would use this command:

```
C:\Program Files (x86)\FullArmor\ADMX Migrator>
  faadmxconv d:\temp\blocksharecreate.adm d:\temp /x
```

where d:\temp is the location to save the generated ADMX file and /x says to also save an ADML file. An ADML file contains the language-specific information used by an ADMX file to allow policy settings to display in the specified language.

InstantDoc ID 97123

—John Savill

Q: Can I upgrade from Windows Server 2008 Server Core to the full Windows 2008?

A: No, you can't upgrade from Server Core to Windows 2008, nor can you downgrade from Windows 2008 to Server Core. If you need to switch versions, you'll need to reinstall.

InstantDoc ID 97225

—John Savill

Darren Mar-Elia (dmarelia@windowsitpro.com)

Mark Russinovich (mark.russinovich@microsoft.com)

John Savill (jsavill@windowsitpro.com)

Ask the Windows IT Pro Community

For answers to more of your Windows server and client systems questions, visit our online discussion forums at www.windowsitpro.com/forums.

Q: How can I run the Link Layer Topology Discovery (LLTD) responder update for Windows XP on Windows Server 2003?

A: The LLTD responder update lets XP computers appear in Windows Vista's Network Map feature. By default, you can't run the LLTP responder update under Windows 2003; Windows 2003 servers will show as unknown location devices. However, you can try to force the update to run by performing these steps:

1. Download the update from www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4f01a31d-ee46-481e-ba11-37f485fa34ea.
2. Attempt to run the update on a Windows 2003 server, but don't click OK to the error about updatebr.inf.
3. At the root of the C drive, you'll see a folder name in the format 7be840d99a33259a5b77a0a9; open this folder and copy the update folder to another location.
4. Click OK to the error message that displays.
5. In the copy of the update folder, right-click update.exe and select Properties.
6. Under the Compatibility tab, select *Run this program in compatibility mode for* and select Windows XP.
7. Click Apply, then click OK.
8. Execute update.exe

I've had mixed results with this working on all Windows 2003 servers, but it's definitely worth a try.

InstantDoc ID 97122

—John Savill

The Case of the Failed File Compression

This is a summary of a popular posting to Mark Russinovich's technical blog (https://blogs.technet.com/markrussinovich/about.aspx), which covers topics such as Windows troubleshooting, technologies, and security. You can read the entire post at https://blogs.technet.com/markrussinovich/archive/2007/08/07/1715181.aspx.

The other day, my colleague Bryce Cogswell tried to use Windows Explorer's Send To Compressed (zipped) Folder feature to package up his latest Process Monitor source code updates to send me. Instead of presenting the compression progress, followed by an opportunity to edit the name of the resulting compressed file, Explorer aborted the compression with a *File not found or no read permission* error.

Bryce was perplexed. The error didn't make sense because he obviously had read permission to the files in the selection, which he'd just finished editing, and compressing files shouldn't involve a search that could result in a file not being found. He showed me the behavior by trying a few more times, all with the same outcome.

To investigate, we launched Process Monitor, reproduced the failure, stopped the capture, and scanned through the thousands of operations in the trace looking for errors. Several hundred events into the trace, we came across a sharing violation error that bore a closer look:

When a process opens a file, it can specify if and how it wants to share the file with other processes while it has the file open. The three types of sharing are read, write, and delete, and each is represented with a flag that a process passes to the CreateFile API. In the operation that failed, Explorer didn't pass any of the flags, indicating that it didn't want to share the file.

For an open to succeed, the sharing mode of the opener must be compatible with the sharing allowed by a process that already has the file opened, so the explanation for the error was that another process already had the file opened. Looking at the trace, we discovered that the open operation immediately preceding the one with the error is an open of the same file by a process named Inort.exe. That confirmed that Explorer's unwillingness to share the file conflicted with Inort having the file open, despite the fact that Inort specified read, write, and delete sharing in its open of the file.

Process Monitor had closed another case: Inort holding the file open when Explorer tried to open it was the cause of the sharing violation and almost certainly the reason for the misleading error message. Next we had to identify Inort so that we could come up with a fix or workaround. Process Monitor also answered that question: eTrust, Computer Associates' antivirus scanner, was apparently opening the file to scan it for viruses but was interfering with the operation of Explorer. Antivirus should be invisible to the system, so the error revealed a bug in eTrust. The workaround was to set a directory filter that excludes the source directories from real-time scanning.

Now I turned my attention back to the inefficiencies of Explorer's compression feature. I captured a Process Monitor trace of the compression of a single file and counted the associated operations. Just for this simple case, Explorer opened the target .zip file 14 times, 12 of those before it had actually created the file and therefore with NOT FOUND results, and performed directory look ups of the target 19 times. It was also redundant with the source file, opening it 28 times and querying the file's basic properties 17 times. It's not like Explorer doesn't give eTrust plenty of opportunities to cause sharing problems.

To verify that Explorer itself was at fault, and not some third-party extension, I looked at the stacks of various events. Zipfldr.dll, the Explorer file compression DLL, was in most of the stack traces, meaning that the compression engine was ultimately responsible for the waste. Further, the number of repetitious operations explodes when you compress multiple files.

Update: I've learned that Microsoft has updated the compression engine in Vista SP1 to perform fewer file operations.

InstantDoc ID 97124

—Mark Russinovich

April 27-30
2008
ORLANDO, FL
Hyatt Regency Grand Cypress

Over 100 in-depth sessions, 75 Microsoft Architect and industry expert speakers, and exciting announcements!

MICROSOFT EXCHANGE Connections 2008

WINDOWS Connections 2008

Office Connections 2008

Dive into the new releases with Microsoft Architects and Industry experts!

Connections raises the bar for IT Conferences, delivering:

- EXPERT SPEAKERS
- UNPARALLELED WORKSHOPS
- DYNAMIC CONTENT
- HOT LOCATION
- EXCITING ANNOUNCEMENTS

CELEBRATE THE NEW RELEASE OF WINDOWS SERVER 2008!

REGISTER TODAY!

THIS EVENT SOLD OUT LAST SPRING!

WinConnections.com ▪ 800-505-1201 ▪ 203-268-3204

EARLY

EARLY BIRD BONUS!

Register and book your room by January 15 and receive a FREE NIGHT at the Hyatt Regency Grand Cypress!
(based on a 3-night minimum stay)

Microsoft® | Windows IT Pro | TechNet MAGAZINE | TECH Conferences Inc. PENTON MEDIA

Choose from:

- 45 white papers at www.windowsitpro.com/whitepapers,
- 37 eBooks at www.windowsitpro.com/ebooks,
- 22 podcasts at www.windowsitpro.com/podcast, and
- 70 web seminars at www.windowsitpro.com/events

to get a jump ahead this Fall.

A multitude of information is just a click away at www.windowsitpro.com

Windows IT Pro

The Final For

Use the original Windows power tool to work with lists of files

I've been talking about the powerful For tool over the past couple months. For can inject power into any command-line utility, letting it transform a command that normally operates on a single file into one that can work on many files. In the first For column, "The Power of For" (InstantDoc ID 96539), I discussed how For can turn a command loose on an entire folder's worth of files, and in the second column, "Counting on For" (InstantDoc ID 96704), I showed you how For's /l option lets you instruct a command to run any number of times.

This month, I show you how For's /f option lets you tell Windows to apply a single command to a specific list of files.

I was sure the answer lay in the For command, so I dived into For's online Help.

For for Files

This For functionality came to mind a few weeks ago while I was reviewing the results of a photo shoot. I'd been snapping dozens of close-up photos of a Snowy Egret from a photographer's blind. I had some good, detailed shots, but most didn't amount to much. I wanted to burn all the photos to a DVD but keep the most useful ones on my computer's hard disk.

You'd think separating out a few pictures would be simple—say, by browsing the pictures in one window while dragging the good ones to another folder. But I needed to devote a lot of screen real estate to the image browser and didn't have enough screen space to hold a couple of Windows Explorer windows on top of that. But I did have enough space for a little Notepad window, in which I could type the names of the files I wanted to keep, leaving me lots of room for the image browser.

I had a folder full of files called C:\newpics, and I had created a text file named keepers.txt that listed the photos I wanted to copy to a folder called C:\goodpics. I wanted to extract each line in keepers.txt and use it as a filename to copy to C:\goodpics. How could I use the Windows command line to accomplish that goal?

I was sure the answer lay in the For command, so I dived into For's online Help, which reminded me of the tool's /f option. Here's the command I came up with:

```
for /f %i in (C:\newpics\keepers.txt) do copy C:\
  newpics\%i C:\goodpics
```

To understand this command, look at the simplified For /f syntax:

```
for /f <variable> in (<name of file listing the
  desired objects>) do <an operation involving the
  variable>
```

For example, to tell For /f to simply display the files that it will copy, I could type

```
for /f %i in (C:\newpics\keepers.txt) do echo %i
```

For /f works its way through keepers.txt by taking one line at a time and putting the contents of that line in a *variable*, a place in memory that I've called "%i." (Any name works, as long as it's prefixed with a percent sign.) Then, For /f performs whatever action you've typed to the right of *do*, replacing the two letters "%i" with the actual value that For has most recently extracted from keepers.txt.

Thus, if I type *pic1.cr2* on the first line, and *pic7.cr2* on the second and final line, For /f would first execute *echo pic1.cr2*, which would cause Windows to just print *pic1.cr2* on the command window, then print *pic7.cr2* on that window and stop.

That's not all For /f can do. Instead of putting a file in the parentheses, you can put a command in there, surrounded by single quotes. For will then execute the command and use each line of the command's output as a line of text to operate on, just as it operated on the lines in keepers.txt.

For can also accept more than one file as input in the parentheses, as in a variation on the first example, featuring both the file keepers.txt and another named keepers2.txt:

```
for /f %i in (C:\newpics\keepers.txt C:\newpics\
  keepers2.txt) do copy C:\newpics\%i C:\goodpics
```

More to For

There's more to For, of course. But I think these three visits with "the original Windows power tool" should give you a pretty good starting point toward your own For experimentation. If you learn only one new command-line tool this year, make it For!

InstantDoc ID 96903

Mark Minasi (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

Did You Know?

You can meet Mark Minasi at the upcoming Windows Connections 2007 conference in Las Vegas, November 5–7. For more information, visit www.winconnections.com.

POCKET THE PROS

Ordering the SQL Master CD is like pocketing a team of SQL experts.

Packed with thousands of articles, bonus content, and loads of expert advice—getting the SQL Master CD is like pocketing your very own team of professional SQL consultants.

And at a fraction of the cost.

Search for articles by keyword, subject, author or issue. Get real-world solutions in lightning-fast time—order the SQL Master CD today.

Only $59.95

POCKET ONE TODAY!

www.sqlmag.com/go/pocketpros 1-800-793-5697

SQL Server magazine

Essential Windows PowerShell Commands

Jump-start your way into scripting with these 10 useful commands

PowerShell is an extensible, objected-oriented scripting language with full support for variables, looping, and pipelining. Microsoft has made PowerShell the scripting framework for almost all of its new products. For instance, PowerShell is integrated into the management consoles for both Microsoft Exchange Server 2007 and the upcoming System Center Virtual Machine Manager 2007. However, while PowerShell represents a revolutionary step in Windows scripting, it's also a very different technology from its predecessors, the Windows command shell and VBScript. PowerShell has a new set of commands (called *cmdlets*) and command syntax that you need to learn. To help you get up to speed, here are 10 essential PowerShell cmdlets.

10 **Get-Help**—The Get-Help cmdlet helps you learn how to use PowerShell. Get-Help not only explains the syntax of commands, but it also provides examples of how to use them. The following example shows how to use Get-Help to learn about the PowerShell Help system itself:

```
get-help
```

9 **cd**—You can use the good ole' cd (Change Directory) command to navigate between folders. Under the covers, cd is an alias for the Set-Location cmdlet. What sets this command apart from the old Windows shell cd command is its ability to navigate the registry. To use cd to go into the HKEY_LOCAL_MACHINE\SOFTWARE subkey, you would enter

```
cd hklm:\software
```

8 **Get-Alias**—PowerShell has more than a hundred different aliases. Plus, you can create custom aliases with the New-Alias cmdlet. Use the Get-Alias cmdlet (or its alias, gal) to list all the PowerShell aliases along with their native counterparts:

```
gal | select name, definition
```

7 **Get-Command**—You use the Get-Command cmdlet to retrieve a list of the hundreds of available commands. PowerShell's support for wildcards helps you narrow your searches. The following example retrieves all the commands that begin with *get*:

```
get-command get*
```

6 **Set-Content**—Set-Content (or its alias, sc) is used to write values to a file. If the specified target file doesn't exist, this command creates it. For example, the following command writes the value "My data" to the file named mynewfile.txt:

```
sc c:\temp\mynewfile.txt -value "My data"
```

5 **Get-Content**—The counterpart to sc is Get-Content (gc). The gc cmdlet is used to read the contents of a file. For example, the following command displays the contents of the file named mynewfile.txt:

```
gc c:\temp\mynewfile.txt
```

4 **Set-ExecutionPolicy**—By default, PowerShell's ability to run scripts is disabled; you can only enter commands at the command line. The Set-ExecutionPolicy cmdlet lets you change the security level for running scripts. To enable PowerShell to run any script, you can enter the following command:

```
set-executionpolicy unrestricted
```

3 **Set-PsDebug**—Although PowerShell doesn't have a full-featured debugger, it does have basic debugging capabilities through the Set-PsDebug cmdlet. Entering the following command will cause a PowerShell script to step through its execution one line at a time:

```
set-psdebug -step
```

2 **Get-Process**—PowerShell has great built-in commands that let you perform many tasks that formerly required resource kits or third-party tools. For example, the Get-Process cmdlet retrieves information about the active processes on a system. Use the following example to list all running processes:

```
get-process
```

1 **Get-Eventlog**—The Get-Eventlog cmdlet retrieves Windows event logs. As with Get-Process, there's no need for additional utilities. The following example shows how you can retrieve the 10 most recent entries from the system event log:

```
get-eventlog -newest 10 -logname system
```

InstantDoc ID 96954

Michael Otey (mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and coauthor of *SQL Server 2005 Developer's Guide* (Osborne/McGraw-Hill).

Jeff James (jjames@windowsitpro.com)
is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*.

At a Glance

Readers Review HOT PRODUCTS

Manage Virtualized Applications

Thinstall Virtualization Suite

We began using **Thinstall Virtualization Suite** because we needed to run several Java Virtual Machine (JVM) versions on a single Windows XP machine. After using Thinstall Virtualization Suite for that purpose for a while, I realized that our internal application development projects could also use it for testing and scaling.

One of the most attractive features of Thinstall is that it doesn't need server or client software to run. You can create standalone .exe files of applications that run without any other software, making Thinstall instances very easy to deploy. Thinstall has made it much easier for us to deploy and move different versions of software throughout our organization.

We've saved a great deal of time (and stress) because we can avoid deploying different workstations to the same user and using virtual machines. VMs aren't bad, but they do require a powerful workstation and some knowledge on the user's part. Thinstall is easy to install and use. I've recommended it to other departments in the government of Quebec, and it has helped them resolve some of the same problems with running JVMs.

There are some features that I hope Thinstall will add in the future. Some sort of a solution builder would let us build an executable application from instructions without needing to capture a setup, and the documentation, especially about fine-tuning the product, could be clearer. Despite these shortcomings, I've enjoyed using Thinstall and enthusiastically recommend it to others.

Reader: Serge Bedard Technology architect specialist
Product: Thinstall Virtualization Suite
Company: Thinstall
Contact: thinstall.com

"Thinstall has made it much easier for us to deploy and move different versions of software throughout our organization."

—Serge Bedard, technology architect specialist

What's Hot continues on page 82

Wanted: Your Real-World Experiences with Products

Have you discovered a great product that saves you time and money? Do you use something you wouldn't wish on anyone? Tell the world in a review right here in What's Hot: Readers Review Hot Products. If we publish your opinion, we'll send you a Best Buy gift card! Send information about a product you use and whether it helps you or hinders you to whatshot@windowsitpro.com.

When it comes to disaster, it's not IF, but WHEN. And too often, it's when you least expect it.

Get High-Availabilty and Disaster Recovery "In-One" With Double-Take®. It is your job to keep servers up, data available and prevent downtime. Failure to protect mission critical data and applications can set your business back by weeks, months or worse. Disaster recovery is now one of the highest IT priorities.

In today's business climate, you have to have a tested plan and reliable tools in place for the moment your server (or site) goes down. Double-Take is that tool. Sold more than all other High-Availability tools combined, it is even certified for W2K Datacenter. No other HA tool is. A whole department sitting on their hands can cost thousands of dollars per minute. The ROI of Double-Take is a no-brainer.

Double-Take delivers real-time data replication combined with fail-over so you have high-availability and disaster recovery for your (virtual) Windows Servers -- safely and securely. This is the reason that hundreds of Fortune 500 companies worldwide use Double-Take to ensure their business continuity. Three levels of data compression allow more data to be replicated and increase performance and scalability.

Double-Take®

Double-Take gives you the peace of mind your data is safe and your job secure. Don't wait. *Download a free 30-day eval copy right now* and start protecting your data and applications.

Certified for Microsoft® Windows Server™ 2003 Standard Edition Enterprise Edition Datacenter Edition

Download your free eval copy today!

Sunbelt Software

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

Secure and Accelerate Network DNS

OpenDNS

Reader:
Dan Orth
Network analyst
Product:
OpenDNS
Company:
OpenDNS
Contact:
www.opendns.com

I work for a restaurant franchising company. Although we oversee the operations of hundreds of restaurants, we maintain a lean IT department of five people that supports both point-of-sale and back-office systems.

I began looking for a publicly available DNS server when I was setting up a client PC. I did a Google search for "Open DNS" and stumbled onto the **OpenDNS** service. Setup of this free service is easy and bulletproof—from start to finish, the process took less than a minute. The product supports dynamically assigned IP addresses, and the Web site even has illustrated walkthroughs of how to set up various popular home routers. After a simple change to our internal DNS structure, we were using the OpenDNS servers.

OpenDNS's antiphishing feature is great. Even with multiple antivirus signature updates and Windows patches, it had been difficult to protect all our users against the latest phishing scams and Microsoft Internet Explorer exploits. OpenDNS lowers our risk by blocking many phishing and potentially dangerous Web sites, and the company maintains the list for us. If you need access to a Web site that's currently blocked, you can simply remove that site from the blacklist.

"OpenDNS lowers our risk by blocking phishing and potentially dangerous Web sites, and the company maintains the list for you."
—Dan Orth, network analyst

The reporting feature can show us all of our top DNS queries by domain, DNS record, and IP address. From the reporting page you can easily block sites, such as ad sites, that are high on your domain list. You can also purge your records from the OpenDNS system if privacy is a concern.

The price for OpenDNS is right, and it functions as advertised. It doesn't get any better than that! I can't think of any improvements the product needs, although I have heard that a new release of the OpenDNS dashboard is in development.

What's Hot continues on page 84

Build your website now for success in the New Year!

At 1&1, we offer affordable web hosting plans for every customer and budget. Set goals for your business next year and let our website solutions help you achieve them.

Sign up today and improve your business with 1&1.

$50 OFF!* First Year

Don´t wait! These specials are only valid through 2007!

DOMAINS

.biz only $2.99 First Year*

ENTERPRISE SERVERS

$200 OFF! First Year**

	1&1 BUSINESS	Yahoo! STANDARD	Go Daddy PREMIUM
Included Domains	3	1	$1.99/year with purchase
Web Space	250 GB	10 GB	200 GB
Monthly Transfer Volume	2,500 GB	400 GB	2,000 GB
E-mail Accounts	2,500 IMAP or POP3	500 POP3	2,000 POP3
Mailbox Size	2 GB	Unlimited	10 MB
Search Engine Submission	✓	✓	Extra charge applies
Website Builder	18 Pages	✓	Freeware
Flash Site Builder	18 Pages	–	–
Photo Gallery	✓	✓	✓
RSS Feed Creator	✓	–	$4.99/month
Ad-free Blog	✓	✓	Freeware
Map & Driving Directions	✓	✓	–
Dynamic Web Content	✓	✓	–
Web Statistics	✓	✓	✓
E-mail Newsletter Tool	✓	$10/month	$3.99/month
In2site Live Dialogue	✓	–	–
Chat Channels	✓	–	✓
Form Builder	✓	✓	–
1&1 Marketing Center	✓	–	–
Premium Software Suite	✓	–	–
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	$9.99	$19.95	$14.99
SPECIAL OFFER FOR 1 YEAR	$50 off*	$14.96 first 2 months	10% off
TOTAL/YEAR	$69.88 ~~$119.88~~	$229.42	$161.88

We offer a variety of hosting packages and servers to fit your needs and budget.

MEMBER OF united internet

Call 1.877.go1and1

Visit us now 1and1.com

1&1

Easily Create PDF Documents

PDFCreator

I work as a PC technician at a small property management company, which has a main office and several remote sites. Nearly a third of the company's employees work remotely.

Our IT infrastructure includes Linux and Microsoft Windows, and we use a variety of software applications to meet our business needs. We needed a way to easily create PDF documents, so I began searching for a low-cost application that would let us do that.

Reader:
John Biondo
PC Technician

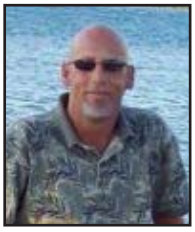
Product:
PDFCreator 0.9.3

Company:
SourceForge.net

Contact:
sourceforge.net/projects/pdfcreator

I specifically needed a product with solid, built-in security. I also wanted to produce documents that could be locked against certain actions—for example, I wanted to be able to prevent anyone without the necessary access rights from editing or printing a PDF.

While searching the Web, I ran across **PDFCreator**, a freeware PDF-creation tool. PDFCreator could do everything I needed and seemed to be the best free PDF creation product out there. Installation was simple and straightforward. The installation file is quite small, making the tool easy to copy (or email) to other computers. I found the program easy to use: To create a PDF from a document, I just select the PDFCreator print driver as I would select a printer in a standard document print window. PDFCreator lets me create PDFs from virtually all Windows programs. Although the settings parameters weren't as straightforward as they could be—I had to guess where to click to change some of the settings the first few times I used the product—and the interface in general could be made easier to use, PDFCreator is a great program that meets our needs.



"The interface in general could be easier to use, but PDFCreator is a great program that meets our needs."

—John Biondo, PC technician

InstantDoc ID 97146

We're ALL New for 2008!

Look inside the new *SQL Server Magazine* and find a completely revised look and feel to help you navigate the magazine with more ease. We've added new authors and features and a renewed dedication to articles concentrating on the information you need to be successful in your profession.

Our editorial focus addresses the entire range of database skills, from beginners to gurus, and addresses IT generalists' need to work with SQL Server as part of other technologies such as SharePoint, Windows Server Update Services (WSUS), MOM, Forefront, and many other technologies.

Take a look inside the new *SQL Server Magazine* and we believe you won't need to look elsewhere.

New layouts and features have been created to deliver a cleaner page highlighting the content you need.

The NEW SQL Server magazine

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.

www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Windows IT Pro UPDATE*
- *Vista UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*
- *.NET Briefing*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server 2005 Express UPDATE*
- *SQL Server Magazine UPDATE*
- *Storage UPDATE*
- *Windows IT Library UPDATE*
- *Connected Home EXPRESS*

www.windowsitpro.com/email

PRO VIP ACCESS

Exchange & Outlook Pro VIP

Discover smart solutions for Exchange and Outlook administrators.

www.exchangeprovip.com

Scripting Pro VIP

Learn how to create more powerful scripts and get tips for automating those tedious administrative tasks.

www.scriptingprovip.com

Security Pro VIP

Discover practical, how-to advice for avoiding and solving security problems.

www.securityprovip.com

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.

www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

www.sqlmag.com

For detailed information about products in this issue of *Windows IT Pro*, visit the Web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

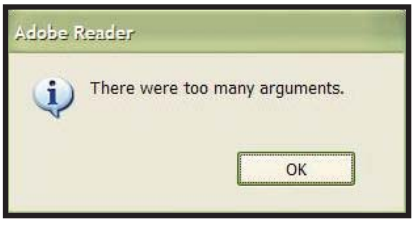
SEND US YOUR INDUSTRY HUMOR! Email your funny screenshots, favorite end-user moments, and humorous IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

STRESSED OUT

Apparently, it's one of those busy days

Or perhaps it's just a mild illness

Then again, maybe everyone is just in a BAD MOOD



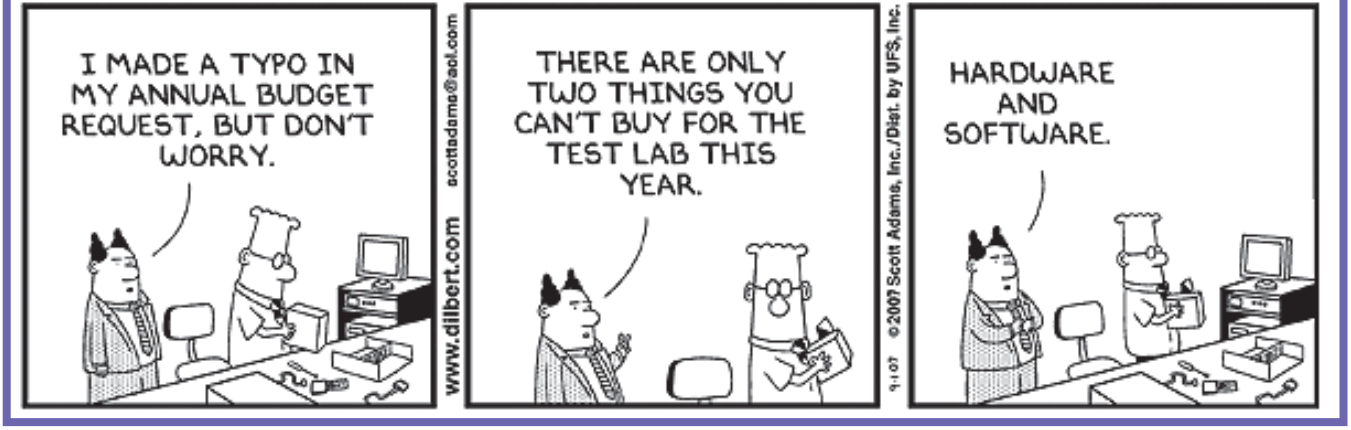
Oops

SEND US YOUR END-USER STORIES

Ever have one of those days when users unintentionally tickle your funny bone? Ever NOT have one of those days?

We've published several hilarious end-user moments in this space over the past year, and we want to hear some more! In 150 words or fewer, send your greatest, funniest, most embarrassing user experience to rumors@windowsitpro.com, and we might just publish it on this page.

DILBERT® by Scott Adams



November 2007 issue no. 159, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Subscriptions in US, $49.95 for one year; in Canada, $59 US currency, plus 6% for GST for one year; in UK £59; in all other countries, US $99. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* P.O. Box 447, Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, P.O. Box 447, Loveland, CO 80539-0447. Printed in the USA. BPA Worldwide Membership Applied for May 2006.

THE I.T. MANAGER'S I.T. MANAGER.

OR $53/ MONTH[1]

Whatever your everyday routine is like, IBM System x3655 Express can help manage routine tasks and save you time. How? It comes with IBM Director, which helps to deploy, monitor, troubleshoot, maintain and optimize your infrastructure from a single screen. It's simple and efficient.

From the people and Business Partners of IBM:
Innovation made easy.

ADVANCED SYSTEMS MANAGEMENT THAT HELPS SAVE YOU TIME AND MONEY.

PN: 7985EBU

- Featuring up to two AMD Dual-Core Opteron™ 2000 Series Processors
- Increased performance-per-watt efficiency with dual-core processing
- IBM Director allows you to manage anywhere from 5 to 5,000 other servers
- Xcelerated Memory Technology means faster access to memory for large memory configurations
- Comes with a 1-year on-site limited warranty[2] on parts and labor

IBM BladeCenter LS21 EXPRESS

PN: 7971E1U

- Featuring up to two AMD Dual-Core Opteron™ 2000 Series Processors
- Up to 32GB of DDR II memory to maximize the amount of memory that can be installed in the ultra-dense blade
- IBM Director allows you to manage servers remotely to help increase uptime and reduce costs
- Integrated SAS controller and connectors for 2.5-inch SFF non-hot-swap SAS HDDs

$3,769

OR $100/ MONTH[1]

(Save $248)

AMD 64 Opteron™

Special offers from IBM Express Servers:

Check out our latest offers. (And they really are our latest offers.) All are designed to help you save money and get the most from your IT investment. Visit our Web site for more details.

IBM express advantage™

ibm.com/systems/itmanager
1 866-872-3902 (mention 6N7AH42A)

1. IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. 2. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit ibm.com/servers/support/machine_warranties or write to: Warranty Information, P.O. Box 12195, RTP, NC 27709, Attn: Dept. JDJA/B203. IBM makes no representation or warranty regarding third-party products or services, including those designated as ServerProven® or ClusterProven.® Telephone support may be subject to additional charges. For on-site labor, IBM will attempt to diagnose and resolve the problem remotely before sending a technician. On-site warranty is available only for selected components. Optional same-day service response is available on select systems at an additional charge. IBM, the IBM logo, IBM Express Advantage, System x and BladeCenter are trademarks or registered trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see ibm.com/legal/copytrade.shtml. AMD, the AMD logo, AMD Opteron and AMD PowerNow! are trademarks of Advanced Micro Devices, Inc. All prices are IBM's estimated retail selling prices as of August 1, 2007. Prices may vary according to configuration. Resellers set their own prices, so reseller prices to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. Prices are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or IBM Business Partner for the most current pricing in your geographic area.

Desktop Authority makes desktop administration easy...

Maybe a little too easy.

DESKTOP AUTHORITY®

Dreaming of a world without logon scripts and sneakernet? Wishing that you could properly manage and secure all of your desktops, laptops, virtual machines and thin clients from one central console? Stop daydreaming and download Desktop Authority today!

- Manage - Configure printer and drive mappings, Outlook profiles and more
- Inventory - Complete hardware and software inventory, custom reporting
- Secure - Comprehensive, centralized patch, spyware, and device management
- Support - Remote management from any Java-enabled browser

Download a 30-day evaluation today and get this Windows Vista eBook free!

www.scriptlogic.com/stopdreaming

SCRIPTLOGIC®